

BITCOIN

Una moneda criptográfica



www.inteco.es
@intecocert



INDICE



AUTORES

Jesús Díaz Vico

Antonio Sánchez Aragó

COORDINACIÓN

Elena García Díez



1 RESUMEN

Bajo el título “BITCOIN: Una moneda criptográfica” esta publicación recoge un análisis técnico de la arquitectura y funcionamiento del sistema de dinero electrónico Bitcoin motivado por el interés que para la comunidad de la seguridad informática puede tener en tanto que supone una aplicación práctica de diferentes instrumentos criptográficos. En consecuencia, no incluye consideraciones de uso más allá de lo que se pueda extraer del breve resumen de uso actual y aceptación cuyo tratamiento pretende solamente aportar una visión de contexto del servicio.

El sistema de dinero electrónico Bitcoin nació con la idea de descentralizar los pagos entre usuarios, eliminando la necesidad de la presencia de instituciones financieras en las transacciones. Aunque no exenta de polémica, esta solución ha demostrado en la práctica que es funcional y válida para la realización de transacciones y su adopción está creciendo en todo el mundo.

Para hacer consistente su funcionamiento, teniendo en cuenta los problemas derivados de una gestión descentralizada, Bitcoin propone una solución basada en redes entre pares (*peer-to-peer*), manteniendo registros de transacciones que no pueden ser alterados sin tener que realizar complicados cálculos matemáticos para recomponer todo el sistema.

No obstante, si se quiere entender su funcionamiento, además de conocer el proceso que se sigue para realizar y validar una transacción, se hace necesario saber la teoría con la que opera y qué tecnología utiliza en su implementación, a fin de conocer además la seguridad que proporciona y qué aspectos hay que tener en cuenta si se está valorando su utilización.

El presente documento empieza con una sección general sobre Bitcoin, introduciendo su historia y los principales eventos de la misma, así como un resumen de sus aspectos más controvertidos, para terminar con una introducción genérica de los principales componentes del sistema y de su modo de funcionamiento. La siguiente sección introduce las primitivas criptográficas y las estructuras de datos con las que se ha construido el sistema, continuando con un análisis detallado del funcionamiento de Bitcoin. En esta sección se sigue el proceso de una transacción, su incorporación en el histórico de transacciones de Bitcoin (conocido como cadena de bloques) y la recompensa a los usuarios que destinan recursos a validarla. Una vez comprendido el funcionamiento, se resumen las propiedades de Bitcoin en cuanto a privacidad y anonimato.

Con esta información, se concluye el documento exponiendo las principales fortalezas y debilidades de Bitcoin. Resumiendo, **sus fortalezas son**:

- El programa de incentivos planteado en la implementación de Bitcoin supone, en forma de recompensas en monedas, una clave para el fomento de la participación de usuarios en la red, actuando como nodos que realizan los cálculos complejos que se requieren.
- La seguridad de Bitcoin es bastante alta puesto que se basa en primitivas criptográficas de seguridad demostrada. Además, su arquitectura evita fraudes como el doble gasto de saldo de los usuarios o la alteración indebida de su “política de funcionamiento”.
- La escalabilidad del sistema, por diseño e implementación, hace que su desempeño en el medio y largo plazo esté garantizado.
- Es un sistema transparente por naturaleza, ya que cualquiera puede comprobar de dónde viene y a dónde va cualquier bitcoin.

Por otro lado, **las debilidades** del sistema se pueden resumir en:

- Aunque la red en sí es segura por diseño, para su funcionamiento se requieren elementos cuya definición e implementación no pertenece a la red propiamente dicha. Por ejemplo, los monederos donde se almacenan las bitcoins dependen del usuario y, por tanto, de sus conocimientos en seguridad para mantenerlos seguros.
- Todas las comunicaciones entre los usuarios se realizan sin cifrar.
- Al tratarse de un sistema basado íntegramente en sistemas de información (sin una moneda física), su implementación está expuesta a posibles errores de programación y vulnerabilidades explotables por usuarios maliciosos para acceder al saldo de los usuarios.
- El hecho de que existan mecanismos independientes al sistema, mediante los cuales se puede reducir notablemente el anonimato de la red, junto con el hecho de ser un sistema transparente, puede suponer una grave amenaza para la privacidad de sus usuarios.
- Además, la propia naturaleza de Bitcoin hace al sistema totalmente dependiente del consumo energético, necesario para realizar los cálculos complejos requeridos para su funcionamiento, con lo que participar en la red supone un coste para los usuarios que a la larga podría no estar compensado por los beneficios obtenidos.



2 BITCOIN[1]: LÍNEAS GENERALES

Bitcoin es una moneda electrónica, un protocolo y un software. La conjunción de estos componentes permite la realización de transacciones casi instantáneas entre pares (*peer-to-peer* o P2P) y, por consiguiente, pagos en todo el mundo con unos bajos costos, o incluso nulos, de procesado de dichas transacciones.

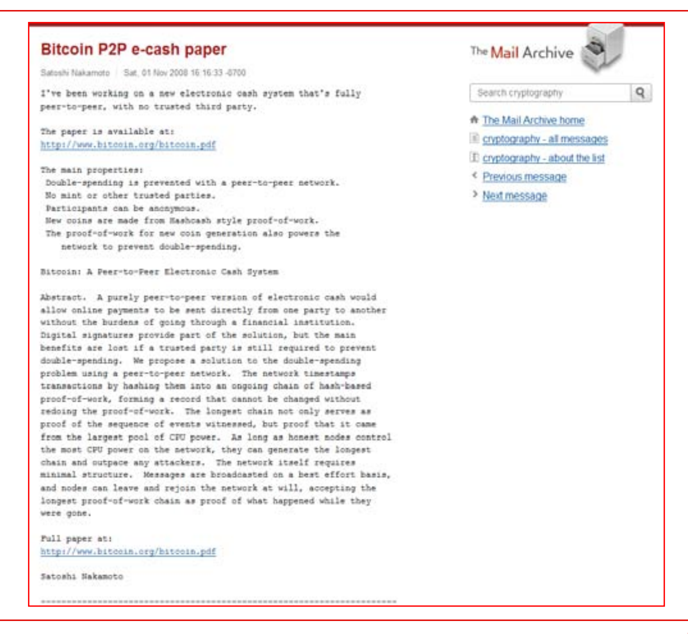
Bitcoin opera bajo tecnología *peer-to-peer* para así evitar depender de una autoridad monetaria central que se encargue de la emisión y el control de dinero. Así, no es posible manipular el valor de las bitcoins o crear inflación produciendo más moneda. La propia red es la que gestiona las transacciones y la emisión de bitcoins, que se generan a través de la llamada minería, de forma controlada y descentralizada.

La utilización de criptografía garantiza la seguridad de las transacciones. Por ejemplo, se puede controlar que sólo el dueño de las monedas pueda gastarlas, y que sólo las pueda utilizar en una única transacción. Las figuras de control y supervisión presentes en los sistemas monetarios de los mercados actuales no existen en bitcoin.

ORIGEN

La primera aparición pública de Bitcoin se produjo en la lista de correo *cryptography*[2], donde un usuario con el pseudónimo «Satoshi Nakamoto» anunció, el 1 de noviembre de 2008, que había estado trabajando en un nuevo sistema de dinero electrónico, resumiendo sus propiedades y el contenido del artículo original que describía su trabajo y que se encontraba disponible en el portal de Bitcoin: http://www.bitcoin.org (ver Figura 1).

Figura 1. Mensaje de «Satoshi Nakamoto» en la lista cryptography.



Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
Double-spending is prevented with a peer-to-peer network.
No mint or other trusted parties.
Participants can be anonymous.
New coins are made from Hashcash style proof-of-work.
The proof-of-work for new coin generation also powers the network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Mail Archive

Search cryptography

The Mail Archive home
cryptography - all messages
cryptography - about the list
Previous message
Next message

Fuente: The Mail Archive

[1] Como convención, en lo que resta de documento se utilizará:
- Bitcoin (con mayúscula inicial) para hacer referencia al sistema completo,
- bitcoin (con minúscula inicial) para referirse a las monedas digitales que se manejan dentro del sistema.

[2] https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

El 11 de febrero de 2009, un perfil creado en el portal *P2P foundation, también* con el nombre de «Satoshi Nakamoto», publicó un mensaje: “Bitcoin open source implementation of P2P currency”[3] (ver Figura 2). En el texto, «Satoshi» daba a conocer el portal oficial de Bitcoin, las características fundamentales de éste, el artículo donde se describía el diseño e, incluso, el cliente inicial con el que comenzar a participar en la red.

Figura 2. Comunicado de «Satoshi Nakamoto».

P2P foundation

The Foundation for Peer to Peer Alternatives

Main | My Page | Members | Videos | Forum | Groups | Blogs | Chat

All Discussions | My Discussions | + Add

Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at

Fuente: P2Pfoundation.

[3] http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

El creador

Por el momento la identidad del creador, o creadores, no ha sido revelada. «Satoshi Nakamoto» es el pseudónimo que fue utilizado por la persona, o el grupo de personas que diseñaron y crearon la red Bitcoin, con el fin de mantener el anonimato y así protegerse a ellos mismos y a la red.

Lo único que se sabe de «Satoshi Nakamoto» son los datos publicados en su perfil del portal *P2Pfoundation*: hombre de nacionalidad japonesa y 38 años de edad (en el momento de publicación de este documento). Sin embargo, no es posible demostrar que estos datos sean reales. Además, dado el diseño de Bitcoin, se le pueden atribuir conocimientos avanzados en criptografía y algoritmos matemáticos.

Hay muchas especulaciones sobre la identidad real que se esconde detrás de este pseudónimo. Una de ellas apuntaría a que se trata de Shinichi Mochizuki, matemático especializado en teoría de números y profesor de la Universidad de Kyoto. Otras especulaciones enlazan la figura de «Nakamoto» con identidades relacionadas con mercados negros y negocios criminales.

En 2011, a través de un correo electrónico a uno de los desarrolladores de Bitcoin, «Satoshi Nakamoto» se desvinculó totalmente del proyecto para dedicarse a otras cuestiones.

UNA NUEVA FILOSOFÍA

Dejando de lado aspectos técnicos, Bitcoin es novedoso porque funciona sin una autoridad central que regule la emisión de moneda, o acepte o deniegue transacciones. Gracias a su arquitectura distribuida, son los usuarios del sistema los que implícitamente toman estas decisiones globales “democráticamente”. Utilizando conceptos que aún no han sido expuestos, es posible aproximarse a esta filosofía a través de dos ejemplos:

1. Como recompensa por colaborar con la red, los usuarios reciben bitcoins (en siguientes secciones se verá cómo se hace). Hasta aquí, puede parecer que los usuarios podrían engañar al sistema para aumentar su recompensa pero, por construcción del sistema, la mayoría de los usuarios tendrán que validar posteriormente esa recompensa. Así, si el usuario la aumentase subrepticiamente, esa acción sería rechazada por el resto.
2. Un usuario *A* hace un pago con una bitcoin *b1* a otro usuario *B*. Para evitar que posteriormente *A* vuelva a utilizar *b1* para pagar a un tercer usuario *C*, en Bitcoin, las transacciones se hacen públicas. Por lo tanto, cuando el resto de la red detecte la segunda transacción, la rechazará, imposibilitando una reutilización de *b1* por parte del usuario *A.*

Como se desprende de los ejemplos anteriores, son los propios usuarios los que toman las decisiones que normalmente corresponden a una única autoridad central. Esto hace que Bitcoin sea una moneda “democrática”. Como en cualquier democracia, su evolución se adapta a lo que la mayoría de la población quiere. No obstante, en este caso no hay una equivalencia de *“un usuario = un voto”*, ya que el peso de cada usuario depende de la potencia de cómputo que éste dedica a la red. Así, la ecuación anterior en Bitcoin, sería más bien *“x% de cómputo = x% de votos”*. Por lo tanto, siempre y cuando más de un 50% de la potencia de cómputo de la red sea controlada por usuarios honestos, la red seguirá la evolución que estos decidan [1, p. 3]. La idea puede contemplarse como una *“democracia ponderada”* en función de la implicación en el sistema.



Visto lo anterior, Bitcoin crea un escenario económico y social totalmente nuevo hasta su aparición. Esto es así porque, de adoptarse Bitcoin, o un sistema equivalente, los gobiernos y autoridades financieras no podrían controlar la evolución del dinero de una forma directa. Sí podrían influenciarla de forma indirecta legislando sobre ella, pero nunca controlar su comportamiento. No obstante, una moneda electrónica no tiene un carácter nacional, sino internacional. Por lo tanto, legislar sobre ella de manera efectiva es más complicado. Además, considerando esta diversidad de escenarios sin precedentes en la teoría económica, los efectos de una aceptación y uso masivos de la moneda son impredecibles.

USO ACTUAL Y ACEPTACIÓN

Como ya se ha mencionado, este documento sólo recoge un análisis técnico de la arquitectura y funcionamiento del sistema de dinero electrónico y no consideraciones de su uso. En este sentido, este resumen de uso y aceptación responde solamente al objetivo de aportar información de contexto al lector. Para conocer implicaciones de su utilización debe consultarse, en cualquier caso, la información aportada por las autoridades bancarias que, como es el caso de la Autoridad Bancaria Europea, disponen recomendaciones específicas sobre el uso de monedas virtuales[4].

El número de empresas y pequeños negocios que aceptan Bitcoin como medio de pago se encuentra en constante aumento. Actualmente, con esta moneda se puede contratar todo tipo de servicios, como telefonía, *hosting* de internet, tarjetas regalo, asesoría legal, turismo, etc. A su adopción han contribuido tanto su ámbito internacional como la sensación de anonimato que transmite, lo que ha propiciado que se utilice para fines ilegítimos, y en situaciones donde las presiones políticas prohíben otros tipos de pagos virtuales.

Sin embargo, su adopción no está exenta de posicionamientos e intentos de control por parte de gobiernos y autoridades. Por ejemplo, el estado de California envió a mediados de 2013 un comunicado a la Bitcoin Foundation, indicándole que estaba obligada a darse de alta como *Money Transmitter* para operar en dicho estado o cesar en su actividad (ver Figura 3) o la decisión del Banco Central de China[5] de no operar con bitcoins en diciembre de 2013. En los últimos días (principios de 2014) Bitcoin ha recibido dos apoyos muy importantes. eBay[6] permitirá transacciones de bitcoins a partir de febrero (de momento sólo en Reino Unido) y Google[7] ha confirmado su interés por esta moneda electrónica.

[4] http://www.eba.europa.eu/documents/10180/16136/EBA_2013_01030000_ES_TRA1_Vinay.pdf
[5] http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html
[6] http://news.cnet.com/8301-1023_3-57617502-93/ebay-to-allow-bitcoin-sales-in-virtual-currency-category/
[7] http://www.forbes.com/sites/andygreenberg/2014/01/22/google-lets-slip-that-its-exploring-possible-bitcoin-integration-plans/



Figura 3. California ordena a la Bitcoin Foundation el cese de sus operaciones.



CNET › News › Internet & Media › Bitcoin Foundation ordered to cease operations in California

Bitcoin Foundation ordered to cease operations in California

Nonprofit organization devoted to promoting the virtual currency is accused of transmitting money without a license.

by Steven Musil | June 23, 2013 5:46 PM PDT
Follow @stevenmusil



The Bitcoin Foundation, a nonprofit devoted to promoting best practices for the virtual currency, has been ordered to cease operations in California.

The California Department of Financial Institutions, which oversees banks, credit unions, and other financial organizations operating in the state, sent a cease-and-desist letter (see below) last month to the foundation accusing it of "engaging in the business of money transmission without a license or proper authorization."

Fuente: CNET

Para prevenir vacíos legales, la *Financial Crimes Enforcement Network* del *Department of the Treasury* redactó una guía para monedas virtuales[8] que, básicamente, legitima este tipo de monedas en Estados Unidos (incluyendo Bitcoin según su funcionamiento descentralizado), pero define las obligaciones que tienen que cumplir sus usuarios y cuándo se considera que se realizan transferencias de dinero y por tanto hay que darse de alta como *Money Transmitter*. Cabe destacar que la Bitcoin Foundation no se dedica a gestionar transferencias de dinero, por lo que no está obligada legalmente a registrarse como *Money Transmitter*.

En el caso de España también está aumentando la adopción de Bitcoin y ya hay multitud de comercios que aceptan esta moneda como pago de sus productos o servicios en gran parte del territorio nacional, como se muestra en la Figura 4 y la Figura 5. En la Wiki de Bitcoin[9] se puede consultar los sitios que admiten bitcoins para los servicios que proporcionan a través de Internet.

[8] http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf
[9] https://en.bitcoin.it/wiki/Trade

Figura 4. Mapa de comercios que aceptan Bitcoins en España.



Fuente: Mercado BITCOIN

Aprovechando la repercusión que está teniendo a nivel internacional, la adopción de esta moneda se utiliza también como fuente de noticias. Así, en el ámbito comercial es una moneda que proporciona alternativas a los tradicionales cobros con tarjeta y que, por otro lado, es cada vez más conocida por el gran público por lo que su adopción puede identificarse como un plus de publicidad y notoriedad.

Figura 5. Noticia sobre el uso de Bitcoins en bares españoles.



RT Actualidad / Economía — http://es.rt.com/pC8 — Imprimir

En tiempos de crisis, monederos virtuales: Bares españoles se suman al uso del bitcóin

Publicado: 26 jun 2013 | 13:33 GMT   Última actualización: 26 jun 2013 | 13:33 GMT

0 0 0 ∞ ∞

Corbis

La moneda virtual bitcóin gana popularidad en España. Decenas de restaurantes y bares empiezan a aceptar este tipo de cambio.

El bitcóin comienza a hacerse un hueco en España más allá de Internet, y la moneda virtual ya funciona en la calle. Además de las transacciones electrónicas, decenas de empresas, especialmente bares y restaurantes, aceptan ya los bitcoines.

Todo sobre este tema

Fuente: RT ¡SEPA MÁS!



Controversia

Dejando de lado los aspectos técnicos, el hecho de ser la primera moneda que no está controlada por ningún estado hace que Bitcoin sea objetivo de mucha controversia. Por un lado, hay quienes la consideran un gran mecanismo para limitar el control de los gobiernos sobre la economía del pueblo. Por otro, es considerada como una fuente de actividades ilegítimas (más o menos, el mismo debate que surge con la red Tor[10]). Además, dado que crea un escenario totalmente nuevo, tampoco está claro qué efectos tendría sobre la economía mundial una adopción masiva de Bitcoin.

Silk Road

Una de las polémicas alrededor de Bitcoin viene del hecho de que suele utilizarse (a veces bajo una injustificada sensación de anonimato) para fines ilegítimos. Por ejemplo, el mercado Silk Road[11], clausurado por el FBI[12], únicamente aceptaba pagos en bitcoins. Cuando se clausuró Silk Road, el FBI se apoderó de parte de la fortuna en bitcoins de Ulbricht (unas 144.336 bitcoins) transmitiéndola a cuentas controladas por el mismo FBI, publicando posteriormente la identidad de estas nuevas cuentas.

Consideraciones económicas

En cuanto al aspecto económico, el valor de Bitcoin viene determinado de la misma forma que otras monedas actuales, como el Euro o el Dólar. Es decir, Bitcoin se puede ver como una divisa fiduciaria, cuyo valor se basa en la confianza que la sociedad deposita en ella. No obstante, el hecho de que las bitcoins no estén controladas por ninguna autoridad hace que las bases de esta confianza sean otras. En el caso de divisas oficiales, es la confianza en el estado o autoridad que la soporta la que determina su valor, y que proporciona mecanismos para evitar que una moneda suba o baje más allá de los límites que considere aconsejables. En el caso de Bitcoin, el valor de cambio de bitcoins[13] con respecto a cualquier otra divisa oficial aumentará conforme la sociedad (usuarios, comerciantes, etc.) acepte pagos con bitcoins, disminuyendo en caso contrario.

Al ser una divisa totalmente diferente a las existentes hasta ahora, además de ser relativamente nueva (con sólo unos años de vida), su "cotización" sufre grandes fluctuaciones debido a que el nivel de confianza en Bitcoin no es tan alto como el de otras divisas oficiales. Por un lado, la confianza en Bitcoin se puede ver afectada por factores técnicos, como el incidente de marzo de 2013[14]. Dicho incidente sucedió concretamente entre el 11 y el 12 de dicho mes, cuando se produjo una actualización en la base de datos utilizada por el principal software de *minado* de bitcoins, "*bitcoind*", que provocó una inconsistencia entre versiones. Esto conllevó la creación de dos cadenas paralelas (un *fork*). Durante un tiempo, una porción de los usuarios de Bitcoin siguió una cadena, mientras el resto siguió la otra, generando esta confusión una depreciación de la moneda, como se muestra en la Figura 6.

---

10 http://inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/red_tor_anonimato_vulnerabilidades

11 http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com

12 http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

13 http://bitcoin.org/en/faq#why-do-bitcoins-have-value

14 http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/



Figura 6. Depreciación de Bitcoin durante el *fork* de marzo de 2013.



La propia construcción de Bitcoin obliga a que estas situaciones se corrijan solas con el tiempo, a través del descarte de una de las dos cadenas, quedando una única cadena válida.

El valor del bitcoin también se ve afectado por robos, timos o situaciones especiales (como el cierre de Silk Road) que introducen incertidumbre o desconfianza en el sistema. La Figura 7 muestra el efecto de dos de los principales eventos puntuales (con una fecha precisa) de este tipo en la historia de Bitcoin: los "*Linode hacks*"[15] en marzo de 2012, donde se robaron aproximadamente 46.653 bitcoins y en la gráfica inferior, el "primer" cierre de Silk Road[16] el 2 de octubre de 2013, donde se confiscaron 144.336 bitcoins a su fundador.

[15] https://bitcointalk.org/index.php?topic=83794.0#post_linode_hacks
[16] https://bitcointalk.org/index.php?topic=83794.0#post_silk_road_seizure



Figura 7. Efecto de los “Linode Hacks” (02/03/2012) y el cierre de Silk Road (02/10/2013) sobre el precio de las bitcoins.

También influyen decisiones tomadas por países o grandes compañías, aunque Bitcoin no es controlada por ningún estado o autoridad. Por ejemplo, la decisión del banco central de China de no operar con bitcoins[17] tuvo el efecto a corto plazo mostrado en la parte superior de la Figura 8, y, probablemente, sea responsable del efecto a medio plazo mostrado en la parte inferior.

[17] http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html

Figura 8. Efectos de la decisión del banco central de China de no operar con bitcoins.



Todo esto pone de manifiesto que el ecosistema Bitcoin está aún en sus inicios y eventos concretos pueden tener efectos más grandes de lo esperado.

Además, hay múltiples incógnitas acerca de los efectos de una adopción a gran escala de monedas virtuales. Ya en 1996, Tatsuo Tanaka, de la Universidad de Columbia, realizó un análisis de las posibles consecuencias en el ya mencionado "Possible economic consequences of digital cash"[18]. Siguiendo el análisis del autor, Bitcoin ahora se encontraría en la fase de expansión, y las posibles fases siguientes serían "confusión" y "organización", con consecuencias por entonces (y aún) bastante inciertas.

Otro comportamiento que se ve amplificado en Bitcoin es que, como indica Paul Krugman, el hecho de que se límite a 21 millones la cantidad total de bitcoins promueve su acumulación, ya que la escasez futura provocará una expectativa de aumento de valor.[19]

Otros problemas

Además de los problemas mencionados, el hecho de que las bitcoins se gestionen de forma electrónica abre nuevas líneas de ataque para software malintencionado. Así, entre el 31 de diciembre de 2013 y el 3 de enero de 2014, Yahoo tuvo un problema de seguridad en los anuncios que servía online. Algunos de estos anuncios contenían malware que permitía la

[18] http://www.isoc.org/inet96/proceedings/b1/b1_1.htm

[19] http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/

instalación de software para minar bitcoins de manera oculta, creando una efectiva botnet de minado[20]. Algunos expertos estiman que este tipo de botnets podrían estar generando $100.000 por día. También empiezan a darse casos de ransomware[21] que exigen recompensas en bitcoins, como es el caso de Cryptolocker (Figura 9).

Figura 9. Mensaje de rescate de Cryptolocker.

CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
20/10/2013
11:11

Time left
71 : 52 : 49

Next >>

PARTICIPANTES

En cuanto a los actores que intervienen en el sistema, se pueden distinguir dos tipos de participantes, que componen dos conjuntos no necesariamente disjuntos:

- **Usuarios normales**: son usuarios del sistema Bitcoin. Compran y pagan bienes y servicios utilizando bitcoins, produciendo transacciones del sistema.
- **Mineros**: son usuarios especiales que dedican potencia de cómputo a validar nuevas transacciones, creando lo que se conoce como bloques de transacciones. Los cálculos que tienen que realizar son muy costosos por lo que se ven recompensados por ellos.

[20] http://www.bbc.co.uk/news/technology-25653664

[21] Ransomware (o Criptovirus): Código malicioso que hace inaccesibles determinados ficheros en el ordenador y coacciona al usuario víctima a pagar un "rescate" (ransom en inglés) para poder acceder a la información. http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Ransomware



Adicionalmente, hay un tercer rol que normalmente se ignora: los **desarrolladores**. El medio principal de Bitcoin es, en definitiva, un software. Como tal, necesita un desarrollo y mantenimiento activos para lo cual es imprescindible un equipo de desarrolladores. Actualmente, el cliente “oficial” de Bitcoin.org está respaldado por 6 desarrolladores[22]. No obstante, al ser un protocolo libre, cualquiera puede crear un cliente de Bitcoin. De hecho, actualmente existen varios[23].

Por tanto, los desarrolladores no pueden tomar decisiones en lugar del sistema, pese a su posición aparentemente central y especialmente influyente, Por ejemplo: los desarrolladores podrían decidir que la recompensa por encontrar un nuevo bloque pasase a ser de 50 a 100 bitcoins, pero si a la mayoría de los usuarios (o más bien a los que proporcionan más de la mitad de la potencia de cómputo) estuvieran en contra de esa decisión, podrían cambiar a otro cliente software de Bitcoin que mantuviese la recompensa que ellos consideran justa. En un caso extremo, cualquiera podría implementar su propio cliente siempre y cuando sea compatible con el protocolo. Así, el servicio de los desarrolladores es imprescindible, pero con una influencia limitada y desde luego mucho menor que en el común de las herramientas software.

CONCEPTOS GENERALES

Para empezar con una idea básica de cómo funciona el sistema, se describen a continuación los conceptos básicos en los que se basa el sistema. Después, se muestra en la Figura 10 un sencillo esquema de cómo se efectúa una transacción en Bitcoin. En secciones posteriores se explicará cada uno de los pasos con más detalle.

Direcciones Bitcoin

Dirección virtual de un usuario que contiene monedas Bitcoin y se utiliza para pagar y recibir pagos, similar a una cuenta de banco. Un mismo usuario puede tener tantas direcciones Bitcoin como necesite y se identifican con una clave pública.

Una dirección Bitcoin es, básicamente, una transcripción de una clave pública. La clave privada asociada sirve para firmar las transacciones y la clave pública sirve para identificar la dirección y validar las firmas.

Monederos

Espacio virtual, equivalente a un monedero físico, donde se almacenan y gestionan direcciones Bitcoin de un usuario y los pagos que se realizan con ellas.

Transacciones

Una transacción es una transferencia de dinero de una dirección Bitcoin *A* hacia otra dirección *B*. Para componer una transacción, el propietario de la dirección *A* firma una transcripción de la dirección *B* (entre otros datos) con la clave privada asociada a la dirección *A*, de forma que la red sabrá que el nuevo propietario legítimo es el dueño de la dirección *B*.

Bloques

Es una estructura que agrupa transacciones. Las transacciones pendientes de confirmar se agrupan en un bloque sobre el que se realiza el denominado proceso de minería.

---

[22] http://bitcoin.org/en/development

[23] Se puede consultar un listado en https://en.bitcoin.it/wiki/Clients.

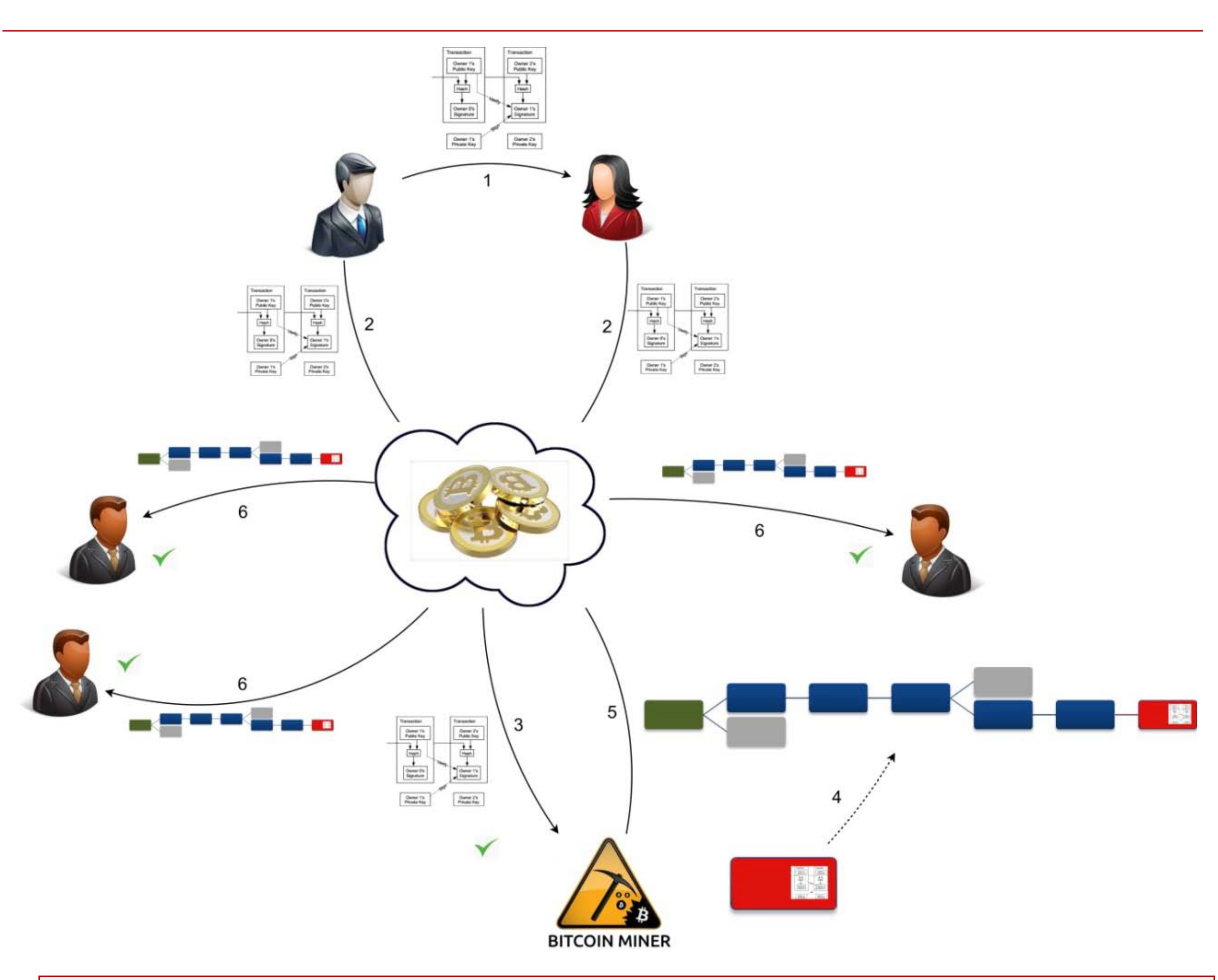
Cadena de bloques

Registro público de las transacciones de Bitcoins validadas en orden cronológico. Cuando un bloque ha sido confirmado, a través de la minería, éste pasa a formar parte de la cadena.

Minería

Proceso de realización de cálculos matemáticos para confirmar transacciones en la red Bitcoin. A través de la minería se pueden crear nuevas bitcoins al mismo tiempo que se confirman transacciones.

Figura 10. Funcionamiento genérico de Bitcoin.



1. *Bob hace un pago en bitcoins a Alice.*
2. *Alice y Bob envían la transacción a la red P2P de Bitcoin.*
3. *Un minero recibe la nueva transacción y la verifica.*
4. *El minero crea un conjunto de transacciones nuevas, incluyendo la transacción del paso 1, y trabaja para confirmarla.*
5. *El minero envía el nuevo bloque de transacciones confirmadas a la red P2P de Bitcoin.*
6. *El resto de usuarios de Bitcoin actualizan su estado incluyendo el nuevo bloque de transacciones, verificando que dicho bloque es válido.*

Como se desprende del esquema anterior, tanto usuarios normales como mineros participan en el sistema de forma activa, aunque son estos últimos los que reciben la mayor carga computacional. Debe observarse también que en ningún momento se necesita la

intervención de una autoridad. Si un minero no acepta procesar una transacción, eventualmente otro minero (o el mismo) lo hará. En la actualidad, dado que la potencia de cómputo necesaria para ejecutar las validaciones necesarias es muy elevada, existen *pools* de mineros. Es decir, agrupaciones de mineros que trabajan conjuntamente para validar un mismo bloque de transacciones para luego repartirse sus beneficios.

OTROS SISTEMAS DE COMERCIO ELECTRÓNICO

Pese a ser la más conocida actualmente, Bitcoin no es el único sistema de dinero electrónico, ni tampoco fue el primero. Esta idea es original de 1985, y fue propuesta por David Chaum en su artículo "*Security without identification: transaction systems to make Big Brother obsolete*" [3]. Desde entonces, se han propuesto multitud de sistemas incorporando mejoras en diferentes aspectos, o sacrificando algunas características en pro de otras. Muestra de ello, en la Wikipedia[24] se puede consultar un listado de monedas electrónicas con una fuerte base en la criptografía (llamadas crypto-monedas) que incluye aproximadamente unos 50 sistemas de dinero electrónico.

En este contexto, como se verá a continuación, Bitcoin destaca porque es el primer sistema que funciona sin una autoridad central. Toda su actividad se "regula" de forma distribuida. En este aspecto, Bitcoin ha sido pionera, y como se dice en la web de *The Economist*[25], pase lo que pase con Bitcoin, este aporte seguramente influenciará notablemente la evolución de cualquier sistema similar.

[24] http://en.wikipedia.org/wiki/List_of_cryptocurrencies

[25] http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital



3 SISTEMA Y PROTOCOLOS

Los sistemas con una complejidad como la de Bitcoin están siempre respaldados por un conjunto de primitivas avanzado. Sin conocer las primitivas, comprender cómo se consiguen muchas de las propiedades anunciadas por el sistema no es posible. Por ello, una vez adquirido un conocimiento general del sistema y cómo funciona, en esta sección se verá en detalle las primitivas fundamentales que toman parte en el mismo.

CONCEPTOS CRIPTOGRÁFICOS

Las primitivas criptográficas de las que Bitcoin hace uso son las responsables últimas de que se consigan las propiedades de seguridad que se persiguen.

Firmas digitales

Bitcoin utiliza el algoritmo ECDSA[26] (Elliptic Curve Digital Signature Algorithm - Algoritmo de Firma Digital de Curva Elíptica) para firmar las transacciones, utilizando los parámetros recomendados por el Standards for Efficient Cryptography Group (SECG), secp256k1 [4]. Las firmas utilizan la codificación DER[27] para empaquetar sus componentes en un único flujo de bytes.

ECDSA ofrece ventajas frente a otros esquemas de firma que lo hacen ideal para su utilización en un protocolo distribuido en Internet, como son:

- Longitudes de clave y de firma muy cortas.
- Generación y verificación de firmas muy rápidas.

Hashes criptográficos

En los cálculos de hashes realizados en Bitcoin se utilizan los estándares SHA-256[28] y, cuando se requiere que el hash sea más corto, RIPEMD-160[29]. Normalmente el cálculo de hashes se realiza en dos fases: la primera con SHA-256 y la segunda, dependiendo de las necesidades de longitud del resultado, con SHA-256 o RIPEMD-160.

```
SHA-256(“Hola”) = E6 33 F4 FC 79 BA DE A1 DC 5D B9 70 CF 39 7C
82 48 BA C4 7C C3 AC F9 91 5B A6 0B 5D 76 B0 E8 8F

SHA-256(SHA-256(“Hola”)) = A7 53 96 6A 11 02 90 57 D6 50 C4 C3
0C 2E 3F 52 8A B6 83 8B 96 C7 BA BB 74 3A EB 9E 3D 6B C4 01

RIPEMD-160(SHA-256(“Hola”)) = F9 3B 68 56 C7 BD 9F 91 97 F7 B5
0F 35 93 09 EE 98 80 92 41
```

[26] http://es.wikipedia.org/wiki/ECDSA
[27] http://en.wikipedia.org/wiki/Distinguished_Encoding_Rules
[28] http://es.wikipedia.org/wiki/Secure_Hash_Algorithm
[29] http://es.wikipedia.org/wiki/RIPEMD-160

Números aleatorios y *nonces*

Los números aleatorios y su generación son pilares fundamentales de la criptografía. Los *nonces* son números aleatorios "especiales" que, en principio, sólo se utilizan una vez (de ahí su nombre, que en inglés viene de ***n**umber used **on**ly **once***), aunque a veces los dos términos se utilizan de forma indistinguible.

En Bitcoin, los números aleatorios y *nonces* se utilizan de forma directa para la generación de bloques. Como se verá a continuación, para obtener un nuevo bloque es necesario encontrar un número aleatorio que satisfaga ciertos requisitos. También se utilizan en Bitcoin, aunque de manera indirecta, como parte del algoritmo de firmas digitales (ECDSA).

Un ejemplo de la importancia de este componente es una vulnerabilidad[30] detectada en agosto de 2013 por la cual, debido a una pobre inicialización del generador de números aleatorios en dispositivos Android, se facilitaba la *deducción* de las claves privadas asociadas a direcciones Bitcoin (ECDSA[31] exige que los números aleatorios utilizados en firmas distintas sean también diferentes).

Pruebas de trabajo

Las pruebas de trabajo (*proofs of work*, en inglés) son el principal componente de Bitcoin responsable de garantizar que la red mantiene un comportamiento legítimo. Brevemente, esta idea hace que validar/calcular nuevos bloques de transacciones conlleve un coste computacional muy elevado, de forma que, para hacerse con el control de la red (y por tanto de qué se valida y qué no), un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir. El principal precursor de esta idea es el método Hashcash[32] ideado en 1997 para evitar el envío de spam.

En concreto, en Bitcoin este control de complejidad en los cálculos para los nuevos bloques se realiza obligando a que el hash de cada nuevo bloque deba comenzar con un número determinado de ceros. Como se verá más adelante, para el cálculo de este hash se combinan datos de bloques anteriores y un *nonce*. Dado que las funciones hash criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes *nonce* hasta encontrar uno que cumpla el requisito preestablecido.

ARQUITECTURA DEL SISTEMA

Los nodos que integran Bitcoin componen un sistema de comunicaciones P2P o *peer-to-peer*. Como ya se ha mencionado, la filosofía aquí es evitar roles de servidor que pudieran evolucionar en, o ser utilizados por, autoridades centrales, gobiernos, etc.

Como todo sistema P2P, Bitcoin dispone de una serie de mecanismos para descubrir nuevos nodos[33] en la red, y mantener una lista actualizada de los mismos. Además, distintos clientes de Bitcoin pueden también ofrecer mecanismos adicionales, como el cliente Satoshi[34]. Entre las principales opciones, destacan los mensajes de tipo *addr* y *getaddr*, mediante los cuales un cliente envía (o solicita) a otro un listado de clientes actualmente conectados a la red. También, en el código de los clientes se suele incluir un listado de

[30] http://bitcoin.org/en/alert/2013-08-11-android
[31] http://en.wikipedia.org/wiki/Elliptic_Curve_DSA#Signature_generation_algorithm
[32] http://en.wikipedia.org/wiki/Hashcash
[33] https://en.bitcoin.it/wiki/Network
[34] https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery



nodos semilla, que se utilizarán para iniciar el proceso de conexión a la red en caso de que el resto de mecanismos fallen. En diciembre de 2013, los nodos semilla incluidos en el cliente "oficial" Satoshi, eran:

- *seed.bitcoin.sipa.be*
- *dnsseed.bluematt.me*
- *dnsseed.bitcoin.dashjr.org*
- *bitseed.xf2.org*

Además de los mecanismos para descubrir otros nodos en la red, hay otros tipos de mensajes de uso frecuente en Bitcoin. Por ejemplo, los mensajes *tx* y *block*, utilizados para enviar datos de transacciones y bloques, respectivamente, de manera que los nodos de la red puedan mantener la sincronía requerida por el protocolo. O los mensajes de tipo *inv*, que se utilizan para anunciar (y retransmitir) nuevas transacciones.

El listado completo de los tipos de mensaje, su definición y explicación, puede encontrarse en la Wiki de Bitcoin[35].

ESTRUCTURAS DE DATOS

En esta sección se verán cómo se construyen los distintos conceptos del sistema a partir de las primitivas criptográficas enumeradas anteriormente.

Direcciones y monederos

Una dirección Bitcoin se compone de un par de claves pública y privada ECDSA (*Elliptic Curve Digital Signature Algorithm*). La dirección se identifica con el hash de la clave pública, al que se añade una suma de verificación. Dicho resumen se codifica en una versión modificada de base 58[36], que básicamente mantiene los ceros a la izquierda cuando realiza la codificación. Así, una dirección se identifica de la siguiente forma:

```
$Version = 1 byte de ceros
$KeyHash = $Version + RIPEMD-160(SHA-256($PublicKey)
$Checksum = SHA-256(SHA-256($KeyHash))[0-3]
$BitcoinAddress = Base58Encode($KeyHash + $Checksum)
```

Al estar identificada por la clave pública ECDSA, todas las operaciones que se realizan con esa dirección deben estar apoyadas por la utilización de la clave privada asociada.

Por lo tanto, los monederos son una agrupación de pares de claves públicas y privadas. En cualquier caso, esto no supone ninguna limitación a que aplicaciones de monederos puedan incluir alguna funcionalidad adicional para realizar otras tareas, como por ejemplo efectuar transacciones.

Transacciones

Las transacciones en Bitcoin son registros firmados digitalmente que cambian el propietario de fondos en bitcoins asignándolos a otra dirección.

[35] https://en.bitcoin.it/wiki/Protocol_Specification#Message_types

[36] La explicación de por qué se usa base 58 en lugar de la típica base 64 se da en https://es.bitcoin.it/wiki/Codificaci%C3%B3n_Base58Check

Para componer una transacción se necesitan los siguientes componentes, formando la estructura que se muestra en la Figura 11:

- **entradas**: esto es, registros que referencian los fondos de transacciones previas
- y **salidas**: registros que determinan el nuevo propietario de las bitcoins transferidas.

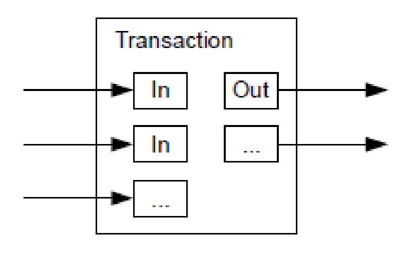
Las salidas se utilizarán nuevamente como entradas de transacciones futuras. Además, siempre se utilizan todas las bitcoins que hay en las direcciones de entrada. Es decir, la suma de todas las entradas no se puede dividir aunque sea mayor que la cantidad a pagar. En este caso, entre las direcciones de salida se incluirá una dirección de devolución, a través de la cual el pagador recibirá "la vuelta".

En concreto, una transacción en Bitcoin está compuesta por los campos mostrados en la Tabla 1[37].

Tabla 1. Campos de una transacción.

Campo	Descripción
Version no	Actualmente 1
In-counter	Número de entradas de la transacción
List of inputs	Lista de entradas de la transacción
Out-counter	Número de salidas de la transacción
List of outputs	Lista de salidas de la transacción
Lock_time	El número de bloque o marca temporal hasta la cual esta transacción está bloqueada.

Figura 11. Transacción.



Fuente: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

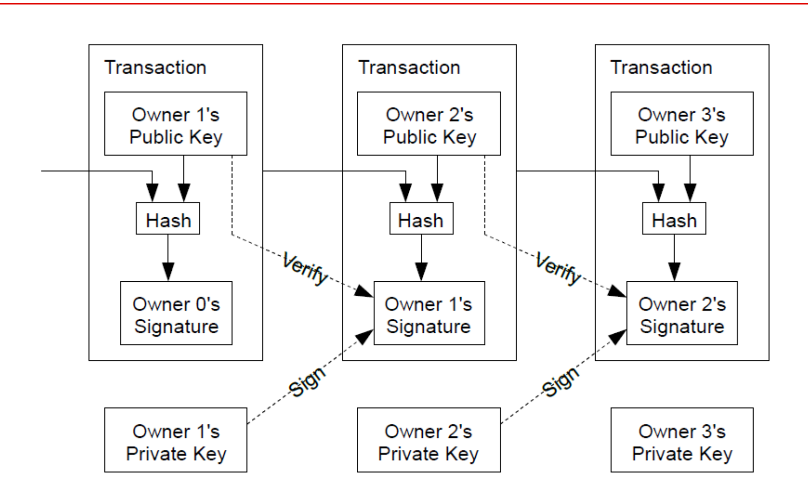
Cada entrada de una transacción es firmada digitalmente por el pagador, lo que desbloquea los fondos contenidos en la dirección asociada a la clave privada utilizada para firmar. Así solamente el usuario que posee la clave privada correspondiente es capaz de crear una firma válida lo que asegura que solamente el propietario del saldo puede utilizarlo. Este proceso se muestra gráficamente en la Figura 12.

En las salidas se especifica, entre otros datos, la dirección del cliente que recibirá las bitcoins y, en caso necesario, una dirección en propiedad del pagador para recibir la vuelta.

[37] https://en.bitcoin.it/wiki/Transactions



Figura 12. Firma de transacciones.



Fuente: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

En una transacción, la suma de sus entradas debe ser igual o mayor que la suma de las salidas. En el caso de que la cantidad de bitcoins de la entrada sea mayor que la de la salida, la diferencia se considera una tasa de transacción, y quien incluya esa transacción en la cadena de bloques puede disponer de esa cantidad. Esta **recompensa** es una manera de motivar a los mineros, que obtienen beneficios por su trabajo en forma de bitcoins, siendo los pagadores los que suelen establecer la tasa a incluir en sus pagos (aunque muchos clientes de Bitcoin utilizan valores por defecto). Por ello, es frecuente que transacciones con tasas (o recompensas) mayores sean procesadas más rápido que transacciones con tasas menores.

Se dispone además de transacciones especiales que suponen la creación de nuevas bitcoins que son generadas a través de la minería por lo que no tienen entradas.

Como curiosidad, cabe destacar que Bitcoin tiene un matiz especial que lo diferencia de las monedas físicas. Cuando alguien roba una moneda física, su propietario legítimo no puede utilizarla, ya que ésta pasa a ser propiedad (ilegítima) del ladrón. En el caso de Bitcoin, si alguien "roba" bitcoins apropiándose de las claves privadas asociadas, el robo no será efectivo hasta que el ladrón transfiera las bitcoins robadas a una cuenta de su propiedad (siempre y cuando la víctima mantenga al menos una copia de las claves privadas). De no hacerlo, dado que el propietario legítimo evidentemente conoce las claves privadas asociadas, éste podrá transferirlas a una cuenta de nueva creación de la cual el ladrón no sepa la clave privada, para así evitar la consumación del robo.

Bloques

Un bloque es un registro que contiene confirmaciones de transacciones que se encontraban pendientes. Aproximadamente cada 10 minutos, en promedio, un nuevo bloque que incluye nuevas transacciones se anexa a la cadena de bloques a través de la minería.

Un bloque está compuesto por los campos mostrados en la Tabla 2[38].

[38] https://en.bitcoin.it/wiki/Blocks



Tabla 2. Campos de un bloque.

Campo	Descripción
Magic no	Valor establecido siempre a 0xD9B4BEF9
Blocksize	Número de bytes que siguen, hasta el final del bloque
Blockheader	Cabecera con metainformación sobre el bloque y la cadena
Transaction counter	Número de transacciones en la siguiente lista
Transactions	Lista de transacciones contenidas en el bloque

De los campos anteriores, destaca en primer lugar la lista de transacciones que incluye las transacciones nuevas que el minero que ha calculado el bloque ha decidido incluir en el mismo. Qué transacciones se incluyen depende principalmente de su prioridad. Dentro de la cabecera se incluyen los campos mostrados en la Tabla 3[39].

Tabla 3. Cabecera de bloque.

Campo	Descripción
Version	Versión de bloque
hashPrevBlock	Hash del bloque anterior
hashMerkleRoot	Hash de la raíz del árbol Merkle
Time	Marca de tiempo de creación del bloque
Bits	Especificiación de la complejidad del bloque
Nonce	Nonce que resuelve la prueba de trabajo

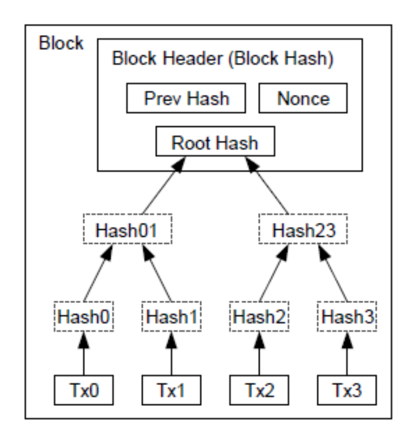
- Los hashes incluidos en los campos segundo y tercero tienen como fin establecer la cadena de bloques cuyo concepto se desarrolla a continuación.
- El campo *Bits* define cual era la complejidad requerida en el momento de generación del bloque para que dicho bloque fuera válido. Esta complejidad es variable en función de la capacidad de cómputo total, de forma que cada bloque se genere, en promedio, cada 10 minutos.
- El valor *Nonce* es el número que resuelve la prueba de trabajo. Concretamente, la prueba de trabajo consiste en calcular el hash (SHA-256) de los seis valores de la cabecera. El hash resultante debe ser menor que el número codificado en *Bits*.

Para optimizar el espacio en disco necesario para almacenar la cadena de bloques, las transacciones que se incluyen en cada bloque se organizan ya en forma de árbol de Merkle (ver Figura 13). Dada la construcción de estos árboles, gran parte de las transacciones incluidas en el árbol pueden ser descartadas o podadas sin comprometer la integridad del bloque.

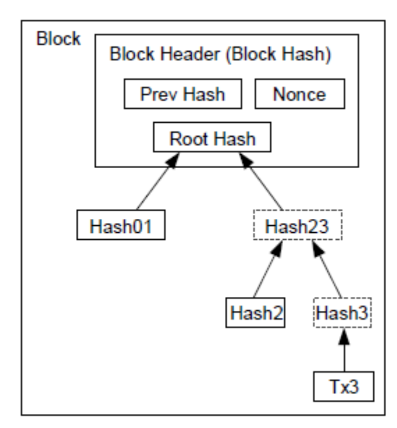
[39] https://en.bitcoin.it/wiki/Block_hashing_algorithm



Figura 13. Bloques y poda de transacciones.



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Fuente: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

Cadena de bloques

La cadena de bloques de la red Bitcoin es una lista creada de forma colectiva con todas las transacciones que han sido confirmadas y validadas por la propia red mediante la inclusión de transacciones en bloques y de estos últimos en la cadena.

Cuando un nodo de la red consigue crear un nuevo bloque, lo transmite al resto de nodos. El resto de nodos verifican que el bloque es correcto, y en caso afirmativo, lo añaden a su cadena y lo difunden. Mediante la difusión del nuevo bloque, éste acabará añadiéndose siempre y cuando no se haya creado otra rama en la cadena de bloques en la que haya participado una cantidad de usuarios con más capacidad de cómputo.

Por la propia naturaleza de la cadena de bloques, se puede extraer el historial de posesión de todas las monedas, siguiendo la lista de transacciones. Así, un usuario no puede reutilizar monedas que ya usó, ya que la propia red rechazará la transacción. Por ejemplo, en Blockchain[40] se pueden ver casos recientes de reutilización de monedas que se han detectado y, convenientemente bloqueado.

Nótese, no obstante, que puede darse el caso de que haya bitcoins reutilizadas de manera no malintencionada. Por ejemplo, por fallos de comunicación masivos, como caídas de redes de comunicaciones, o cuando se crean ramas en la cadena, conteniendo cada una aproximadamente la mitad de la potencia de cálculo del sistema.

Por ello, es buena práctica esperar un tiempo determinado para confirmar una transacción y, por lo tanto, que el receptor de la bitcoin pueda considerar el pago como recibido. Por defecto, los clientes más extendidos incluyen un tiempo de espera de 6 bloques. Es decir, hasta que no se hayan validado 6 bloques desde el que incluyó la transacción, no se considera el pago como realmente efectuado. Dado que el tiempo medio de generación de bloques es de uno cada 10 minutos, esto supone que las transacciones tardan en confirmarse aproximadamente una hora.

Por último, la cadena de bloques, en lo que a estructura de datos se refiere, se establece mediante los campos *hashPrevBlock* y *hashMerkleRoot* de cada bloque vistos anteriormente.

[40] https://blockchain.info/double-spends



EL PROTOCOLO

En esta sección se verá con detalle cómo funciona el sistema Bitcoin. Empezando por la primera piedra del complejo sistema, el *bloque génesis*, y siguiendo su funcionamiento a través de una transacción concretada sobre los conceptos vistos hasta ahora.

La primera piedra: el bloque génesis

Para iniciar Bitcoin, se generó un primer bloque al que se denomina **bloque génesis** y cuya recompensa por resolverlo fue de 50 bitcoins, las primeras monedas de la red.

Figura 14. Bloque génesis.

```
{
"hash":"0000 0000 0019 d668 9c08 5ae1 6583 1e93 4ff7 63ae 46a2 a6c1 72b3 f1b6
0a8c e26f",
"ver":1,
    "prev_block":"0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
                  0000  0000 0000 0000",
"mrkl_root":"4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212
             7b7a fded a33b",
"time":1231006505,
"bits":486604799,
"nonce":2083236893,
"n_tx":1,
"size":285,
"tx":[
  {
  "hash":"4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212 7b7a
          fded a33b",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":204,
  "in":[
    {
    "prev_out":{
    "hash":"0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
            0000 0000 0000",
    "n":4294967295
    },
    "coinbase":"04 ffff 001d 0104 4554 6865 2054 696d 6573 2030 332f 4a61 6e2f
                3230 3039 2043 6861 6e63 656c 6c6f 7220 6f6e 2062 7269 6e6b 206f
                6620 7365 636f 6e64 2062 6169 6c6f 7574 2066 6f72 2062 616e 6b73"
    }
  ],
  "out":[
    {
    "value":"50.00000000",
    "scriptPubKey":"04 678a fdb0 fe55 4827 1967 f1a6 7130 b710 5cd6 a828 e039
                    09a6 7962 e0ea 1f61 deb6 49f6 bc3f 4cef 38c4 f355 04e5 1ec1
                    12de 5c38 4df7 ba0b 8d57 8a4c 702b 6bf1 1d5f OP_CHECKSIG"
    }
  ]
  }
],
"mrkl_tree":[
  "4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212 7b7a fded
   a33b"
]
}
```

Titular de The Times



Como curiosidad, comentar que el creador insertó en uno de sus parámetros (el parámetro *coinbase*, mostrado en las líneas 30 a 32 de la Figura 14 en formato hexadecimal) el siguiente mensaje:

> *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*

Este texto, que hace referencia a la portada del diario The Times, se incluyó en el bloque génesis como prueba de que la red empezó a funcionar después del 3 de enero de 2009.

El proceso de una transacción

Como se ha visto en la definición de transacciones, una transacción cuenta con varios campos, entre ellos, las entradas y las salidas. La Figura 15 muestra el volcado de una de las transacciones incluidas en el bloque 278569 (fechado en el 4 de enero de 2014).

- En la línea 2 se muestra el hash de la transacción, es decir, el resto de campos combinados y pasados por la función SHA-256.
- Las líneas 3 a 6 siguen el formato definido anteriormente:
  - "`ver`": el número de versión actual (1).
  - "`vin_sz`": el número de entradas de la transacción. En este caso, 3.
  - "`vout_sz`": el número de salidas de la transacción. En este caso, 2.
  - "`lock_time`": indica hasta cuándo estará bloqueada esta transacción. Al tener valor 0, la transacción no está bloqueada.

  Además, la cabecera incluye el número de bytes que ocupa la transacción, en este caso, 523.
- Entre las líneas 8 y 39 se incluye la lista de entradas:
  - Para cada entrada, se especifica su origen mediante la estructura "`prev_out`". Esta estructura incluye:
    - El hash de la transacción que la produjo como salida. Por ejemplo, el hash de la transacción que produjo la primera entrada es `7303c1f3ea…` (línea 11).
    - Además, se especifica con el campo "`n`" el número de salida de entre todas las salidas que de dicha transacción (empezando a contar desde 0). Por ejemplo, la primera entrada fue la segunda salida de la transacción anterior, ya que se indica "`n: 1`" (línea 12).
  - Cada entrada incluye también un campo "`scriptSig`", que contiene dos valores muy importantes, separadas entre sí por un espacio:
    - La firma de la transacción. Por ejemplo, "`30450…ace01`" (líneas 14 a 16) en la primera entrada.
    - La clave pública del pagador asociada a la dirección de la entrada. Por ejemplo, "`0260…caba`" (líneas 16 y 17) en la primera entrada.



Figura 15. Volcado de la transacción 3acbc0f5209ab34fa55f91c497bf9d66bd1cb5f93991a6cab258f696319a707f.

```
1   {
2   "hash":"3acbc0f5209ab34fa55f91c497bf9d66bd1cb5f93991a6cab258f696319a707f",
3   "ver":1,
4   "vin_sz":3,
5   "vout_sz":2,
6   "lock_time":0,
7   "size":523,
8   "in":[
9     {
10    "prev_out":{
11      "hash":"7303c1f3ea6d6a0d47acf52caa62474de072a7be052f8f9c9e75c5f7a5357189",
12      "n":1
13    },
14    "scriptSig":"30450221009f66e972ba44157debcc6767e785b5c6c8272e1d4a1d307a6bef7f318
15                 a5648b5022011c3d3728dfc842eeb8494759705972e22a371737254896df13dc2a0
16                 c6119ace01 02608d4b6e1819212e9bc2921315ef1dcdddb5f262f007ff5f92130f3
17                 2efb4caba"
18    },
19    {
20    "prev_out":{
21      "hash":"3b5976b29f32a7f8ad920becd18da1511a14f9318a3bcf1705dc9cd6235d44e5",
22      "n":1
23    },
24    "scriptSig":"304502200af267ac7ca972b5da64fc547bb68bd160d06fffea2b53e1d357132d6d7
25                 0f5480221008f4b2077909c88cc37bbbc3b4701c0ffb6154a01c632d20335034dca
26                 30b8c79f01 02597c2f2743aa205115b5fe3a3fae3a51a638cc58efec47c0081fd03
27                 5c82d1715"
28    },
29    {
30    "prev_out":{
31      "hash":"5f90d3d02fc0ba4ee6fcbd8a4642d509a2b3ffcbebd4a4294cd3b75406bd0fcc",
32      "n":0
33    },
34    "scriptSig":"30460221008ad5baee1e2a967aff997826b3a93006e4eca08784a4d09ec40f70278
35                 f0fa902022100b6e89c5815cf61e980b56c760fab9afaff66bec968b9a9bb6ef1f9
36                 aee508293201 02608d4b6e1819212e9bc2921315ef1dcdddb5f262f007ff5f92130
37                 f32efb4caba"
38    }
39  ],
40  "out":[
41    {
42    "value":"20.00000000",
43    "scriptPubKey":"OP_DUP OP_HASH160 f91bd2092b0ed5dcc3f989fe664d39f40bc1be99
44                    OP_EQUALVERIFY OP_CHECKSIG"
45    },
46    {
47    "value":"0.40870000",
48    "scriptPubKey":"OP_DUP OP_HASH160 3e5f4b5a6ca82a3e494ce0fc9422a3c68b9e7d17
49                    OP_EQUALVERIFY OP_CHECKSIG"
50    }
51  ]
52  }
```


Es destacable que no se incluye el importe de la transacción en ninguna de las entradas. Esto es así porque se transfieren todos los fondos de cada una de las direcciones de entrada, a las direcciones de salida.

Finalmente, se incluye la lista de salidas (líneas 40 a 51), en este caso, dos:

- En el campo "`value`" se especifica el valor transferido a cada salida. Por ejemplo, en primera se transfiere un valor total de 20 bitcoins (línea 42), mientras que en la



segunda, se transfiere un total de 0.4807 bitcoins (línea 47).

- También, cada salida cuenta con un campo "`scriptPubKey`" (líneas 43 y 44 para la primera salida, y 48 y 49 para la segunda) que incluye varios datos en una misma cadena. El más importante es el hash que aparece, que identifica la dirección de salida. Por ejemplo, en la primera salida, la dirección es "`f91b…be99`" (línea 43).El resto de valores son comandos en un lenguaje de scripting propio de Bitcoin. Posiblemente, una de las dos direcciones sea la del cliente que recibe el pago, y la otra pertenezca al pagador, y se utiliza para recibir el cambio. No obstante, desde una única transacción, de forma independiente, es difícil establecer cuál es cuál. En este ejemplo, se asumirá que la primera dirección es la dirección del cliente que recibe el pago, y la segunda es la dirección de recepción del cambio.

Recordando el proceso de una transacción en Bitcoin, en el caso de los datos reales de la transacción que se acaba de analizar, lo que ocurre es lo siguiente:

1. Las direcciones previas relacionadas con esta transacción son:
    1. La segunda salida ("`n: 1`") de la transacción "`7303…7189`".
    2. La segunda salida ("`n: 1`") de la transacción "`3b59…44e5`".
    3. La primera salida ("`n: 0`") de la transacción "`5f90…0fcc`.
2. El pagador utiliza las claves privadas correspondientes a las claves públicas "`0260…caba`", "`0259…1715`" y "`0260…caba`" para generar las firmas digitales que demuestran que se están transfiriendo los fondos de cada una de las direcciones de entrada a las direcciones de salida. Las firmas producidas son, respectivamente: "`3045…ce01`", "`3045…9f01`" y "`3046…3201`". Nótese que la primera y tercera clave públicas coinciden. Esto significa que el pagador utiliza el mismo par de claves para ambas direcciones.
3. El pagador especifica en las salidas que, la dirección "f91b…be99" va a recibir 20 bitcoins y la dirección "`3e5f…7d17`" va a recibir 0.4807 bitcoins. El pagador entonces difunde la transacción al resto de la red. Eventualmente, ésta llegará a un minero que decida incluirla en el siguiente bloque. En este caso, la transacción que se ha analizado se incluyó en el bloque 278569 (fechado en el 4 de enero de 2014). En la sección siguiente se verá cómo.

Minando un nuevo bloque

Como ya se ha mencionado, la minería es el proceso de creación de nuevos bloques, y es una tarea muy costosa a nivel computacional.

En la Figura 16 se muestra el contenido del bloque 278569, que será analizado para explicar el proceso de minería de manera detallada.

La cabecera del bloque mostrado incluye los siguientes campos:

- "`ver`" (línea 3): con la versión de bloque, en el bloque bajo análisis, la 2.
- "`prev_block`" (línea 4): el hash del bloque anterior, con el valor "`00000000000000010...a1e5`".
- "`mrkl_root`" (línea 5) el hash de la raíz actual del árbol Merkle, con el valor "`ea7f…7c8d`"
- "`time`" (línea 6): el tiempo Unix de creación del bloque, "`1388837339`".



- “bits” (línea 7): la complejidad del bloque actual, establecida a “419628831”.
- “nonce” (línea 8): el nonce que resuelve la prueba de trabajo, en este caso “1183905159”.

A continuación, se incluye información relativa a las transacciones incluidas en el bloque. En concreto:

- Campo “n_tx” (línea 9): número de transacciones incluidas en el bloque, en este caso “267”.
- Campo “size” (línea 10): el número de bytes que siguen.
- Campo “tx” (líneas 11 a 22): la lista de transacciones, que tendrán un aspecto similar al que se ha visto en la sección anterior (en la Figura 16 se omiten por facilitar la lectura).

Finalmente, entre las líneas 23 y 27 del volcado mostrado en la Figura 16, también se incluye el contenido del árbol de Merkle (del que se han omitido varias líneas intermedias), que permite verificar que el bloque está correctamente incluido en la cadena de bloques.

Figura 16. Volcado del bloque 278569.

```
1  {
2    "hash":"00000000000000010d3c12aba4e30310a7ab44062a9acef2a2ef796ceaa0a313",
3    "ver":2,
4    "prev_block":"00000000000000010f506a248cb023addb43b06874f77e0e5fd78036af0ea1e5",
5    "mrkl_root":"ea7f525d9e7ab577063abf00142e183022396e4b54ce7a813769172a48337c8d",
6    "time":1388837339,
7    "bits":419628831,
8    "nonce":1183905159,
9    "n_tx":267,
10   "size":146355,
11   "tx":[
12     {
13       "hash":"573d733ad6f6b7203ebee4e266cee48df8ac1dc876185cdd1a5b4b188a1cb242",
14       "ver":1,
15       "vin_sz":1,
16       "vout_sz":434,
17       "lock_time":0,
18       "size":14879,
19       "in":[ … ],
20       "out":[ ... ]
21     }, …
22   ],
23   "mrkl_tree":[
24     "573d733ad6f6b7203ebee4e266cee48df8ac1dc876185cdd1a5b4b188a1cb242",
25     ...
26     "ea7f525d9e7ab577063abf00142e183022396e4b54ce7a813769172a48337c8d"
27   ]
28 }
```

Cabecera (líneas 3–8) · Transacciones (líneas 11–22) · Árbol Merkle (líneas 23–27)

La parte interesante concerniente a la minería la componen los campos “bits”, “nonce” y el primer valor de todos, “hash”. El hash del bloque se calcula utilizando los campos de la cabecera[41], es decir, en este caso, se utilizarían los valores “2”, “00000000000000010...a1e5”, “ea7f…7c8d”, “1388837339”, “419628831” y

[41] https://en.bitcoin.it/wiki/Block_hashing_algorithm



“1183905159”, correspondientes a los campos “ver”, “prev_block”, “mrkl_root”, “time”, “bits” y “nonce” respectivamente.

Para determinar qué hashes serán considerados válidos, se utiliza el campo “bits”. En concreto, este campo es una versión codificada del máximo valor que puede tomar el hash del bloque para ser considerado válido. Para obtener dicho límite, hay que convertir el valor contenido en el campo “bit” a hexadecimal, en el ejemplo, 419628831 en base 10, o 0x1903071F en base 16, y aplicar la siguiente fórmula[42]:

$$0x03071F * 2 ** (8 * (0x19 - 3)) = 0x3071F00000000000000000000000000000000000000000000$$

Cualquier hash con un valor inferior a dicho número hexadecimal, será válido. Aplicando la función SHA-256 a los valores de cabecera mencionados anteriormente (usando la codificación adecuada), se obtiene el valor especificado en el parámetro “hash”, en concreto “00000000000000010d3c12aba4e30310a7ab44062a9acef2a2ef796ceaa0a313”, que es menor que el valor límite y es, por tanto, un hash válido. Nótese que todos los campos que intervienen en el hash son fijos excepto el “nonce”. Así, este campo es el que hace que un hash sea válido o no, y es el que los mineros tienen que ir variando hasta encontrar un hash válido. Obviamente, cuanto menor sea el límite, más difícil es encontrar un nonce válido (porque se reducen los números que satisfacen la fórmula).

Recompensas

Dado que calcular nuevos bloques es muy costoso, el minero o los mineros que encuentren nuevos bloques reciben una recompensa.

Esta recompensa puede recibirse por dos medios. Por un lado, Bitcoin tiene establecido un límite máximo de 21 millones de bitcoins y hasta que se llegue a ese límite, la generación de cada nuevo bloque es recompensada con una cantidad predefinida de bitcoins *nuevas*. Por ejemplo, hasta noviembre de 2012, se recompensaba con 50 bitcoins a cada nuevo bloque. Desde entonces, la recompensa es de 25, estimándose que se reducirá a la mitad hacia 2016.

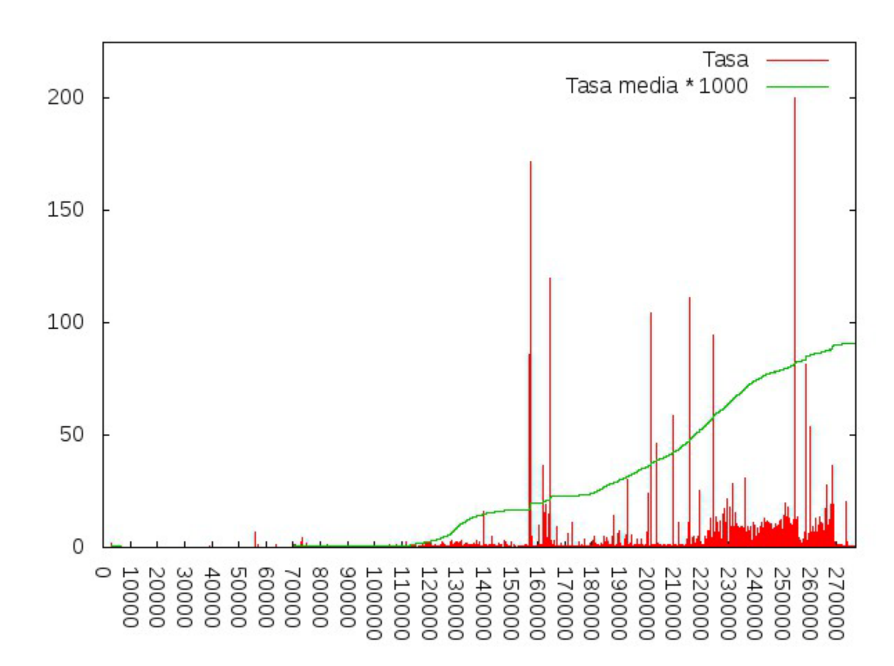
Por otro lado, para mantener una motivación similar para los mineros pese al decrecimiento de las recompensas (que eventualmente llegará a cero), existen las tasas de transacción, mediante las cuales, los usuarios “donan” parte del dinero implicado en una transacción al minero que la valide. En la Figura 17 se muestra la evolución de las tasas de transacción desde el comienzo de Bitcoin. La línea roja muestra la tasa de transacción de cada bloque, mientras que la línea verde muestra la media acumulada hasta el número de bloque asociado, multiplicada por mil (para que sea visible en la misma gráfica). Por ejemplo, alrededor del bloque número 255.000, hubo un bloque por el que se pagó aproximadamente 200 bitcoins (parece un caso extremadamente excepcional), mientras que hasta el bloque 120.000 aproximadamente, la tasa de transacción era prácticamente nula. En cuanto al valor medio de las tasas, se observa cómo va aumentando de manera suave pero constante. Por ejemplo, alrededor del bloque 150.000, la tasa de transacción media rondaba los 0.02 bitcoins (20 / 1000), mientras que alrededor del bloque 270.000 la tasa de transacción media es de unos 0.09 bitcoins. Nota: como fuente de datos para obtener esta gráfica se ha

[42] https://en.bitcoin.it/wiki/Difficulty



utilizado la propia cadena de bloques de Bitcoin, obteniendo los datos contenidos en cada bloque utilizando la herramienta *blockparser*[43].

Figura 17. Evolución de las tasas de transacción en Bitcoin.



Un detalle adicional, que permite aumentar la resistencia de Bitcoin frente a atacantes o ante situaciones atípicas, es que las recompensas (incluyendo nuevas monedas) obtenidas a través del minado no se pueden gastar hasta que se hayan añadido 100 bloques nuevos a la cadena. Esta política es útil por ejemplo para evitar casos en los que se genera un bloque (por tanto creándose nuevas monedas) y el minero que lo creó utiliza algunas de esas bitcoins, pero posteriormente el bloque es descartado por no pertenecer a la cadena más larga. El término utilizado para este concepto es "*100-block maturation time*"[44].

Confirmación de la transacción

Aunque una transacción nueva haya sido incluida en un bloque y dicho bloque en la cadena, inicialmente puede ser posible que esa modificación sea revertida. Esto podría pasar cuando se crean dos ramas inicialmente válidas, lo cual puede ocurrir por diversos motivos. Por ejemplo, como ocurrió en el incidente de marzo de 2013 comentado en la sección de Consideraciones económicas; o si dos mineros reportan dos nuevos bloques válidos al mismo tiempo. Este último escenario se muestra en la Figura 18.

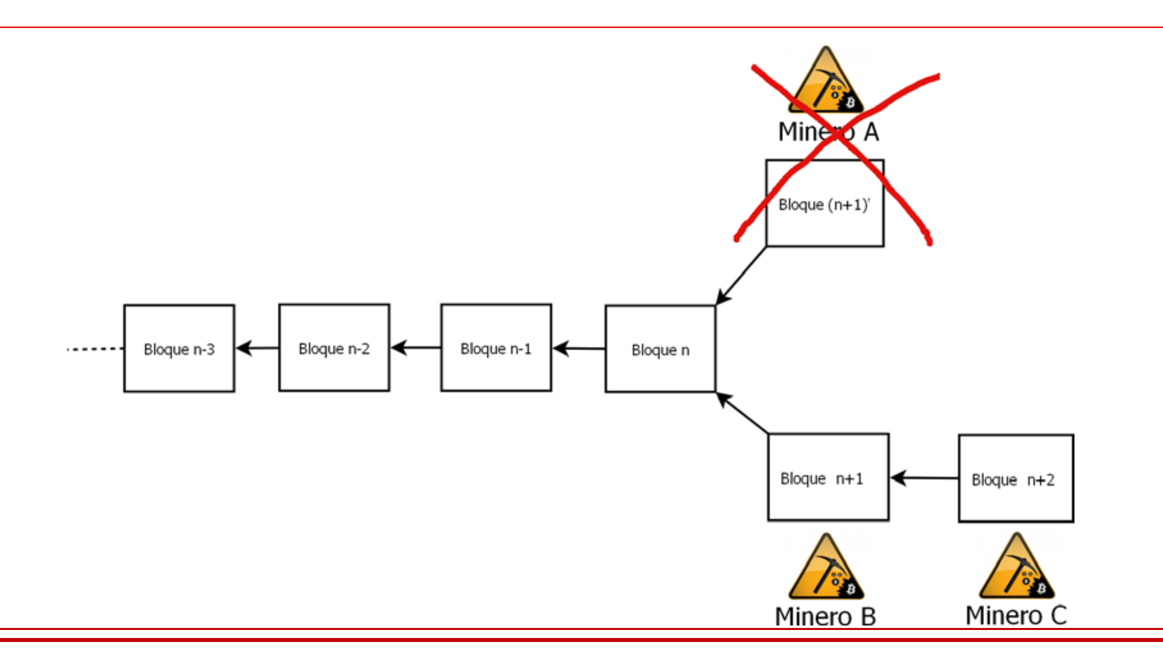
[43] https://github.com/znort987/blockparser
[44] https://en.bitcoin.it/wiki/Block_chain

Figura 18. Creación de ramas alternativas en la cadena de bloques.

Minero A
Bloque (n+1)'
Bloque n-3
Bloque n-2
Bloque n-1
Bloque n
Bloque (n+1)''
Minero B

Al generarse dos ramas distintas, cada una de ellas será respaldada inicialmente por una cantidad determinada de mineros, que irán extendiéndola. Cuanto más similares sean las capacidades de cómputo de las ramas, más se tardará en resolver la ambigüedad, aunque eventualmente una de las ramas recibirá un nuevo bloque antes que la otra y prevalecerá sobre ella, como se muestra en la Figura 19.

Figura 19. Resolución de ramas alternativas.



No obstante, esto es un caso posible y dar por válida una transacción no respaldada por nuevos bloques no es buena idea. Por ello, es aconsejable esperar un número determinado de bloques hasta considerar una transacción como confirmada. El número de bloques puede



variar dependiendo de la cantidad involucrada en la transacción, y obviamente, en función de las consideraciones personales. Normalmente, se considera que tras 6 bloques nuevos, la transacción será difícilmente revertida y, por tanto, se puede considerar confirmada. Nótese que la probabilidad de revertir una transacción decrece exponencialmente por cada nuevo bloque que la respalda.

4 ANONIMATO Y PRIVACIDAD EN BITCOIN

Bitcoin es generalmente interpretado como un sistema que garantiza el anonimato de los usuarios que operan en él[45]. No obstante, desde la sección de privacidad[46] de la misma Wiki de Bitcoin[47], se dice que:

> *Bitcoin is often perceived as an anonymous payment network. But in reality, Bitcoin is probably the most transparent payment network in the world. [..] Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous.*

Es decir, Bitcoin es un sistema con una gran transparencia en sus transacciones fundamentalmente porque el histórico global de transacciones está disponible para cualquiera. En este aspecto, debe notarse que pese a la posibilidad de podar transacciones para optimizar espacio de almacenamiento, siempre hay nodos (públicamente accesibles), llamados *archival nodes*, que contienen el histórico completo. Esto es así para poder verificar con total certeza que no ha habido irregularidades.

Si bien es cierto que internamente no se relacionan las direcciones Bitcoin con identidades reales, eventualmente un usuario que quiera realizar un pago en bitcoins, tendrá que proporcionar algún dato identificativo a quien le proporcione el servicio en cuestión, por lo que su identidad quedará enlazada con la dirección que utilice para el pago[48]. En este caso, a menos que se haya hecho una gestión perfecta de las direcciones Bitcoin, la dirección de pago se podrá utilizar para trazar otras direcciones relacionadas. Por tanto, son varias las fuentes que concluyen que es imposible que una dirección Bitcoin permanezca completamente anónima. Como se ha visto en la sección de Controversia, a través del caso de Silk Road, este tipo de trazados ya ha ocurrido en operaciones reales.

Quizá parte de la confusión general sobre el anonimato proporcionado por Bitcoin deriva de una afirmación hecha en el artículo original por «Satoshi Nakamoto» [1]:

> *[..] privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.*

No obstante, desde el punto de vista criptográfico, esto no se refiere *literalmente* a que la identidad del propietario de dichas claves permanezca anónima. Más bien se refiere a que dichas claves no contienen una identidad real "dentro" de ellas. A pesar de ello, como se ha avanzado y se verá con más detalle a continuación, esto no evita que sea posible (incluso probable, en ocasiones), deducir la identidad real de quien maneja una dirección Bitcoin.

---

[45] Ver por ejemplo: http://www.wired.co.uk/news/archive/2013-05/7/bitcoin-101 ó http://shop.wikileaks.org/donate#dbitcoin

[46] http://bitcoin.org/en/protect-your-privacy

[47] http://bitcoin.org/en/protect-your-privacy

[48] Es costumbre y buena práctica en estudios de privacidad considerar que se pierde la misma en el momento en que se revela algún dato considerado privado a una entidad diferente a aquella cuya privacidad está bajo análisis.



En cualquier caso, cabe destacar que Bitcoin en sí mismo, como sistema, no requiere la introducción de datos identificativos y que, a diferencia de los sistemas de comercio tradicionales, no existe una autoridad central a la que se pueda preguntar por la identidad real del propietario de una cuenta.

Trazando usuarios en Bitcoin

A continuación se hace un repaso sobre los principales métodos de des-anonimización sobre Bitcoin.

Trazado basado en análisis de tráfico

Como informan los autores de "*An Analysis of Anonymity in the Bitcoin System*" [5], citando a Dan Kaminsky, es posible mediante el análisis del tráfico TCP/IP descubrir la identidad de quien realiza un pago en Bitcoin. Debido al diseño de Bitcoin, la primera persona en anunciar una transferencia será, con alta probabilidad, el pagador de la misma. Por lo tanto, descubriendo quién fue el primero en publicarla, se podrá deducir con gran probabilidad quién es el pagador de dicha transacción y por tanto el propietario de las direcciones de entrada utilizadas.

Sobre cómo hacerlo, Dan Kaminsky comenta[49] que no es costoso establecer una conexión con todos los nodos activos en un instante específico de tiempo. Esto puede variar con el tiempo, de igual manera que lo puede hacer el volumen de la red de Bitcoin. En concreto desde la charla de Kaminsky (de 2011) la red ha crecido notablemente. Según el servicio *getaddr* de Bitnodes[50], a 14 de enero de 2014, había aproximadamente 127.741 nodos conectados. En cualquier caso, aunque no sea posible establecer conexiones con todos los nodos, siempre será posible hacer ataques dirigidos, analizando segmentos de red que probablemente estén relacionados con objetivos específicos.

También es destacable que este ataque está basado en la naturaleza de Bitcoin (que el primero en anunciar una transacción probablemente sea el pagador). Por ello, Bitcoin por sí mismo tiene difícil evitar este ataque. Para solucionarlo, no obstante, bastaría con utilizar algún sistema de anonimización de las comunicaciones, como Tor.

Trazado basado en heurísticas

Otro tipo de análisis que destaca bastante es el que se basa en las relaciones que se pueden establecer entre direcciones que, en algún momento, aparecen como entradas comunes a una transacción. Y es que, dada la construcción de Bitcoin, el hecho de que una entidad utilice varias direcciones Bitcoin como entrada a una misma transacción es garantía de que dicha entidad controla las claves privadas asociadas a dichas direcciones. Por lo tanto, parece seguro asumir que todas esas direcciones pertenecen a la misma persona. Aplicando este principio y otros similares, varios estudios desarrollan heurísticas para reducir el grado de anonimato de los usuarios de Bitcoin [6] [7]. Por ejemplo, los autores de "*Evaluating User Privacy in Bitcoin*" [6] estiman que aproximadamente el 40% de los usuarios de Bitcoin podrían ser identificados las utilizando heurísticas del estudio.

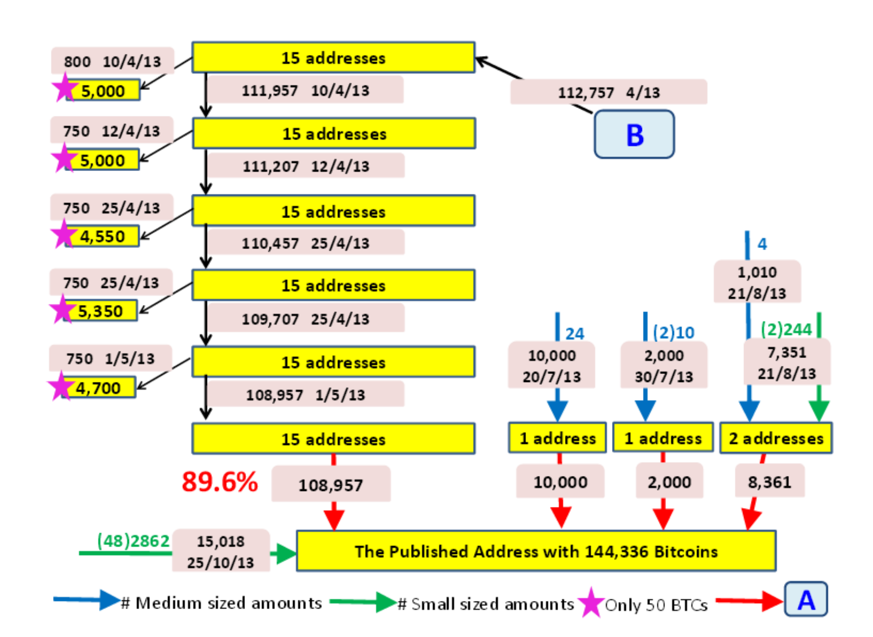
Un resultado bastante llamativo, obtenido aplicando este tipo de medidas, es el que publicaron a finales de 2013 los investigadores Ron y Shamir [2] en el que fueron capaces de establecer una relación entre el fundador del Silk Road y quien probablemente fuera uno de los creadores de Bitcoin. La Figura 20 muestra parte del análisis de los investigadores. Poco después de publicarse esta investigación, el propietario de las bitcoins a las que se

[49] http://dankaminsky.com/2011/08/05/bo2k11/
[50] http://getaddr.bitnodes.io/chart/nodes/



llegó tras realizar este trazado [desmintió esta conexión][51]. No obstante, la capacidad de trazado probada por los investigadores sigue siendo completamente válida.

Figura 20. Trazado de las monedas del fundador de Silk Road.



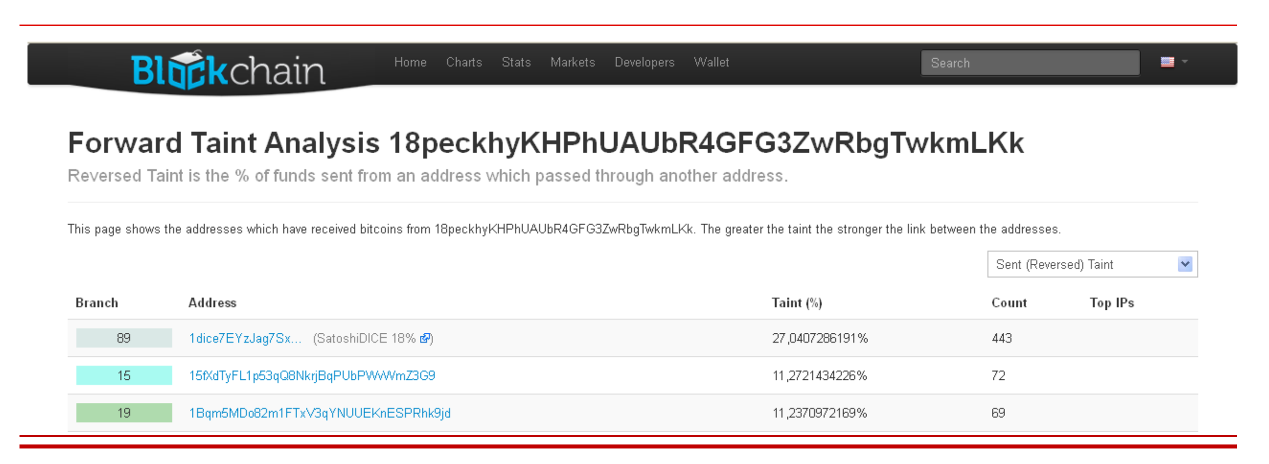
Fuente: "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth", [2]

Otro ejemplo bastante ilustrativo de este tipo de análisis está accesible directamente desde la Web de Blockchain https://blockchain.info/taint/ donde, continuando dicha URL con el hash de una dirección, se muestra un lista de direcciones relacionadas con ella, incluyendo un valor de *taint*, como se muestra en la Figura 21. Dicho valor indica la correlación entre la dirección consultada y otras, incluso incluyendo la identidad a la que están asociada (ver por ejemplo la primera transacción de la figura, en la que se indica que la primera dirección pertenezca a "*Satoshi Dice*", una web que sortea bitcoins, con un 18% de probabilidad).

[51] http://blog.dustintrammell.com/2013/11/26/i-am-not-satoshi/



Figura 21. *Ejemplo de* taint analysis de Blockchain.



No obstante, de igual forma que el trazado de usuarios mediante tráfico TCP/IP se puede mitigar, también es posible reducir la efectividad de estos ataques a la privacidad. Para ello, es necesario mantener una partición[52] de las direcciones Bitcoin controladas por una misma persona, controlando que nunca se utilizan direcciones de dos subconjuntos distintos como entradas de una misma transacción.

Servicios de *mixing*

Como medida avanzada para aumentar el anonimato, y por tanto la privacidad, de los usuarios que participan en Bitcoin, existen servicios adicionales conocidos como *mixing services* o servicios de mezclado [8], basados en los servicios homónimos propuestos en 1981 por David Chaum para anonimizar comunicaciones [9]. Dichos servicios poseen un conjunto de direcciones Bitcoin a las cuales los usuarios pueden transferir bitcoins. Tras un determinado retraso para evitar ataques basados en análisis de tiempo, el usuario volverá a recibir sus bitcoins desde otra dirección que no está relacionada con la suya. En [8], se analizan tres de estos servicios utilizando métricas preestablecidas para estimar el grado de anonimato obtenido, concluyendo que dos de ellas (Bitcoin Fog[53] y Blockchain Send Shared[54]) proporcionan un alto grado, mientras la tercera (BitLaundry[55]) no lo consigue.

En cualquier caso, el uso de estos servicios requiere depositar mucha confianza en ellos, lo cual va parcialmente en contra de la filosofía de Bitcoin de no requerir el uso de autoridades de confianza. Esto es así por dos motivos: primero, hay que confiar que dichos servicios no mantienen un log de transacciones que puedan filtrarse; segundo, se han dado casos de servicios deshonestos que no devuelven las bitcoins recibidas, como informan los autores de [7] sobre el servicio BitMix (aparentemente inactivo ahora).

52 http://es.wikipedia.org/wiki/Partici%C3%B3n_%28matem%C3%A1tica%29
53 http://www.bitcoinfog.com/
54 https://blockchain.info/es/wallet/send-shared
55 http://app.bitlaundry.com/



5 CONCLUSIONES: FORTALEZAS Y DEBILIDADES

Como fin a este análisis técnico de la arquitectura y funcionamiento del sistema de dinero electrónico, se resumen a continuación las principales fortalezas y debilidades del sistema Bitcoin.

FORTALEZAS

Confianza distribuida

En los modelos tradicionales, la confianza se deposita completamente en una autoridad o entidad que controla toda la información. En Bitcoin, por el contrario, no existe dicha autoridad, si no que la información es gestionada por todos los usuarios. De esta forma, siempre y cuando más de la mitad de los usuarios del sistema sean honestos, las "normas" establecidas por el sistema no podrán saltarse por ninguno de los usuarios deshonestos.

Incentivos

Por convención, mientras no se llegue al límite de 21 millones de bitcoins, cuando un minero construye un nuevo bloque, es recompensado con una cantidad predefinida de bitcoins. De esta manera se incentiva a los nodos para que soporten la red, y se define una manera de crear y distribuir monedas, puesto que no existe una autoridad central que las acuñe.

Los incentivos pueden también proporcionarse a través de tasas por la validación de transacciones, de forma que el usuario que crea un bloque válido recibe un pago con una parte del saldo involucrado en la transacción validada.

Criptografía

El uso de un sistema criptográfico asimétrico fuerte, como es ECDSA, y de algoritmos de hashing robustos, como SHA-256, garantiza la integridad actual del sistema. Pero teniendo en cuenta que la capacidad de cómputo aumenta considerablemente año tras año, además de producirse nuevos avances en la teoría criptográfica/criptoanalítica, no es descabellado pensar que los algoritmos que hoy son seguros, no lo serán mañana. Es por ello que el sistema está diseñado de forma que se pueda modificar el sistema criptográfico a utilizar, utilizando el mismo protocolo de comunicación entre pares y de gestión de transacciones. Simplemente se trata de permitir, a partir de un momento determinado y si fuera necesario, que las nuevas transacciones utilizarán un sistema criptográfico diferente[56].

Escalabilidad

Como se ha visto anteriormente, Bitcoin funciona con comunicaciones *peer-to-peer*, por lo que su crecimiento se basa en la adhesión a la red de nuevos nodos.

Sin embargo, no hay que olvidar que el funcionamiento de Bitcoin se basa en la criptografía, y específicamente en el uso de ECDSA (obviando las operaciones sobre RIPEMD-160 y SHA-256 que son lo suficientemente rápidas como para no tenerlas en cuenta en cuanto a escalabilidad). Cálculos realizados sobre la implementación de ECDSA indican que se pueden realizar unas 8.000 verificaciones de firmas digitales por segundo en un procesador

[56] Esta filosofía de diseño que "ignora" las primitivas criptográficas específicas que se puedan utilizar se conoce como modelo Dolev-Yao. Este modelo asume que las primitivas criptográficas subyacentes son perfectas, lo que permite poder diseñar el sistema centrándose únicamente en los protocolos de comunicación



de escritorio actual. Los últimos datos de Bitcoin Watch muestran que se producen alrededor de 2.500 transacciones por hora, cerca de 0,7 transacciones por segundo. La red necesitaría un crecimiento espectacular para alcanzar los límites teóricos.

De cara a la escalabilidad, se debe tener en cuenta además las necesidades de almacenamiento. Bitcoin mantiene un listado de todas las transacciones que se han realizado en la red desde su comienzo. Esto implica que la cadena de bloques crecerá en el tiempo indefinidamente. No obstante, recuérdese que la mayoría de transacciones pueden ser eliminadas de la cadena de bloques, por lo que el tamaño de la cadena disminuye notablemente.

Según el documento original de descripción de Bitcoin [1], donde se indica que la cabecera de un bloque tendría un tamaño de 80 bytes, y teniendo en cuenta la generación de bloques cada 10 minutos, la cadena crecería 4,2MB por año (80 bytes * 60minutos/10minutos * 24 horas * 365 días).

Transparencia

Como se afirma en su propia wiki, Bitcoin es probablemente el sistema de pagos electrónicos más transparente que existe. Esto es debido a que cualquiera puede consultar el histórico completo de transacciones, y saber de dónde viene o a dónde ha ido cualquier moneda en concreto. Esto, por ejemplo, permite “marcar” monedas que han sido robadas o que se haya probado que han intervenido en actividades ilegítimas, de forma que cualquier posible receptor de las mismas pueda rechazarlas posteriormente. No obstante, esta posibilidad no es siempre vista con buenos ojos[57].

DEBILIDADES

Vulnerabilidades

A lo largo del tiempo de vida de la red Bitcoin, se han descubierto vulnerabilidades en las diferentes implementaciones que han aparecido, y que pueden ser explotadas por usuarios maliciosos para obtener diversos beneficios; desde el robo de bitcoins o producir doble gasto de moneda, hasta provocar el mal funcionamiento de la propia red. En el Anexo II se puede consultar una tabla con las 5 vulnerabilidades más graves que se han detectado hasta la fecha de publicación de este informe. La lista completa de vulnerabilidades en Bitcoin se puede consultar en la *Open Sourced Vulnerability Database*[58].

Robo de monederos

La definición de monedero, per se, no incluye que éste se cifre, puesto que es una medida de seguridad que queda del lado del usuario. Por defecto la mayoría de monederos se guardan sin cifrar, lo que ha posibilitado que aparezca malware específico que se dedica al robo de monederos. Algunos monederos empiezan a incluir la opción de que se almacenen cifrados.

En este sentido cabe prestar especial atención a las copias de seguridad de los monederos. Debido al funcionamiento del sistema, a través de una copia de seguridad con una contraseña antigua se pueden obtener las bitcoins de una versión más reciente del monedero.

---

[57] http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/
[58] http://osvdb.org/search?search[vuln_title]=bitcoin



Tráfico sin cifrar

Las comunicaciones entre los diferentes pares se realizan “en claro”, es decir, sin cifrarlas. Aunque este hecho no tiene un impacto fuerte sobre Bitcoin (cualquier usuario puede conectarse a la red y por tanto tener acceso a todas las transacciones), es una cuestión a tener en cuenta, puesto que según las necesidades de los usuarios se deberían implementar medidas de seguridad complementarias.

Según la implementación actual de Bitcoin, un usuario malintencionado puede espiar el tráfico de otro usuario e identificar las transacciones que realiza este último, simplemente cotejando las transacciones que llegan al usuario y las que salen.

Consumo de energía

El valor de un Bitcoin está totalmente relacionado con el consumo energético. La minería se realiza en base a operaciones computacionales, y para ello los equipos tienen que estar conectados y en funcionamiento, con el consumo de energía que eso representa.

Teniendo en cuenta la dificultad creciente que la red introduce en la minería de bitcoins, y el coste de la energía eléctrica, a la larga podría no resultar rentable dedicarse a la minería, por lo que las tasas aplicadas a las transacciones deberían crecer para mantener la sostenibilidad del sistema. Sin embargo, este mismo hecho podría hacer que los usuarios abandonasen la red por otras con menores costes.

Anonimato y privacidad

Pese a que Bitcoin como tal no requiere introducir datos identificativos para hacer uso del mismo, es posible reducir notablemente el grado de anonimato proporcionado por el sistema mediante métodos independientes basados en la propia construcción y funcionamiento del sistema, por lo que muchas veces son difícilmente evitables. Aunque se pueden mitigar mediante una gestión concienzuda de las direcciones de Bitcoin, hacerlo de forma efectiva puede ser complicado.

Teniendo esto en cuenta, dado que la cantidad de bitcoins contenidas en cualquier dirección es una información pública, podría deducirse el dinero que posee una persona específica cuya identidad haya sido comprometida, o también de dónde llegó dicho dinero y cuál fue su destino. Sin lugar a dudas, esto supondría un grave peligro para la privacidad (e incluso la integridad) de las personas en caso de adoptarse Bitcoin de forma masiva.



REFERENCIAS

ARTÍCULOS RELACIONADOS

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] D. Ron and A. Shamir, "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?," 2013. [Online]. Available: http://eprint.iacr.org.

[3] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," vol. 28, no. 10, 1985.

[4] Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters," 2010.

[5] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," 2011.

[6] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating User Privacy in Bitcoin," vol. Financial Cryptography and Data Security, 2013.

[7] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," 2013.

[8] M. Möser, "Anonymity of Bitcoin Transactions," Münster Bitcoin Conference, 2013.

[9] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84-88, 1981.

OTRAS REFERENCIAS

- *Aviso a los consumidores sobre las monedas virtuales*, accedido el 27/01/2014, http://www.eba.europa.eu/documents/10180/16136/EBA_2013_01030000_ES_TRA1_Vinay.pdf.
- *The Mail Archive post: Bitcoin P2P e-cash* paper, accedido el 27/01/2014, https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.
- *Bitcoin open source implementation of P2P currency*, accedido el 27/01/2014, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
- *Portal de Bitcoin*, accedido el 24/01/2014, http://www.bitcoin.org.
- *Possible Economic Consequences of Digital Cash*, accedido el 24/01/2014, http://www.isoc.org/inet96/proceedings/b1/b1_1.htm.
- *Bitcoin is evil*, accedido el 27/01/2014, http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/.
- *La banca china no operará con bitcoins*, accedido el 24/01/2014, http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html.
- *eBay to allow Bitcoin sales in 'virtual currency' category,* accedido el 24/01/2014, http://news.cnet.com/8301-1023_3-57617502-93/ebay-to-allow-bitcoin-sales-in-virtual-currency-category/.
- *Google Lets Slip That It's Exploring Possible Bitcoin Integration Plans*, accedido el 24/01/2014, http://www.forbes.com/sites/andygreenberg/2014/01/22/google-lets-slip-that-its-exploring-possible-bitcoin-integration-plans/.
- *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, accedido el 24/01/2014, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.
- *Bitcoin Trade*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Trade.
- *Red Tor: anonimato y vulnerabilidades*, accedido el 24/01/2014, http://inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/red_tor_anonimato_vulnerabilidades.
- *Silk Road: Not Your Father's Amazon.com*, accedido el 24/01/2014, http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com.
- *End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market*, accedido el 24/01/2014, http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/.
- *Why do bitcoins have value?*, accedido el 24/01/2014, http://bitcoin.org/en/faq#why-do-bitcoins-have-value.

- *Bitcoin Network Shaken by Blockchain Fork*, accedido el 24/01/2014, http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/.
- *Linode Hacks*, accedido el 24/01/2014, https://bitcointalk.org/index.php?topic=83794.0#post_linode_hacks.
- *Silk Road Seizure*, accedido el 24/01/2014, https://bitcointalk.org/index.php?topic=83794.0#post_silk_road_seizure.
- *Yahoo malware enslaves PCs to Bitcoin mining*, accedido el 24/01/2014, http://www.bbc.co.uk/news/technology-25653664.
- *Bitcoin development*, accedido el 24/01/2014, http://bitcoin.org/en/development.
- *Bitcoin Clients*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Clients.
- Notable cryptocurrencies, accedido el 24/01/2014, http://en.wikipedia.org/wiki/List_of_cryptocurrencies.
- *Mining digital gold*, accedido el 24/01/2014, http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital.
- *ECDSA*, accedido el 24/01/2014, http://es.wikipedia.org/wiki/ECDSA.
- *DER Encoding*, accedido el 24/01/2014, http://en.wikipedia.org/wiki/Distinguished_Encoding_Rules.
- *SHA*, accedido el 24/01/2014, http://es.wikipedia.org/wiki/Secure_Hash_Algorithm.
- *RIPEMD-160*, accedido el 24/01/2014, http://es.wikipedia.org/wiki/RIPEMD-160.
- *Android Security Vulnerability: 11 August 2013*, accedido el 24/01/2014, http://bitcoin.org/en/alert/2013-08-11-android.
- *Elliptic Curve DSA, Signature generation algorithm*, accedido el 24/01/2014, http://en.wikipedia.org/wiki/Elliptic_Curve_DSA#Signature_generation_algorithm.
- *Hashcash*, accedido el 24/01/2014, http://en.wikipedia.org/wiki/Hashcash.
- *Bitcoin Network*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Network.
- *Satoshi Client Node Discovery*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery.
- *Bitcoin Protocol Specification: Message Types*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Protocol_Specification#Message_types.
- *Bitcoin: Codificación Base58Check*, accedido el 24/01/2014, https://es.bitcoin.it/wiki/Codificaci%C3%B3n_Base58Check.
- *Bitcoin Transactions*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Transactions.
- Bitcoin blocks, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Blocks.
- *Block Hashing Algorithm*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Block_hashing_algorithm.
- *Blockchain: Gastos Duplicados*, accedido el 24/01/2014, https://blockchain.info/double-spends.
- *Bitcoin Difficulty*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Difficulty.
- *Blockparser*, accedido el 24/01/2014, https://github.com/znort987/blockparser.
- *Blockchain*, accedido el 24/01/2014, https://en.bitcoin.it/wiki/Block_chain.
- *A simple guide to Bitcoin*, accedido el 24/01/2014, http://www.wired.co.uk/news/archive/2013-05/7/bitcoin-101.
- *Wikileaks dontations*, accedido el 24/01/2014, http://shop.wikileaks.org/donate#dbitcoin.
- *Bitcoin: Protect your Privacy*, accedido el 24/01/2014, http://bitcoin.org/en/protect-your-privacy.
- *Black Ops Of TCP/IP 2011*, accedido el 24/01/2014, http://dankaminsky.com/2011/08/05/bo2k11/.
- *Bitnodes*, accedido el 24/01/2014, http://getaddr.bitnodes.io/chart/nodes/.
- *I Am Not Satoshi,* accedido el 01/04/2014, http://blog.dustintrammell.com/2013/11/26/i-am-not-satoshi/
- *Partición de un conjunto*, accedido el 24/01/2014, http://es.wikipedia.org/wiki/Partici%C3%B3n_%28matem%C3%A1tica%29.
- *Bitcoin Fog*, accedido el 24/01/2014, http://www.bitcoinfog.com/.
- *Blockchain Send Shared*, accedido el 24/01/2014, https://blockchain.info/es/wallet/send-shared.
- *BitLaundry*, accedido el 24/01/2014, http://app.bitlaundry.com/.
- *Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community*, accedido el 24/01/2014, http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/.
- *OSVDB*, accedido el 24/01/2014, http://osvdb.org/search?search[vuln_title]=bitcoin.



ÍNDICE DE FIGURAS Y TABLAS

FIGURAS

TABLAS

ANEXO I – ÁRBOLES MERKLE

Los árboles Merkle son árboles binarios de hashes. Un árbol binario es una estructura de datos, en forma de árbol como su nombre indica, donde cada nodo puede tener como máximo dos hijos (árbol binario). Para entender su funcionamiento se utilizará como referencia la figura siguiente:

Figura 22: Ejemplo de árbol Merkle.

Fuente: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

Así, en el caso específico del ejemplo, los nodos se consiguen de la siguiente manera:

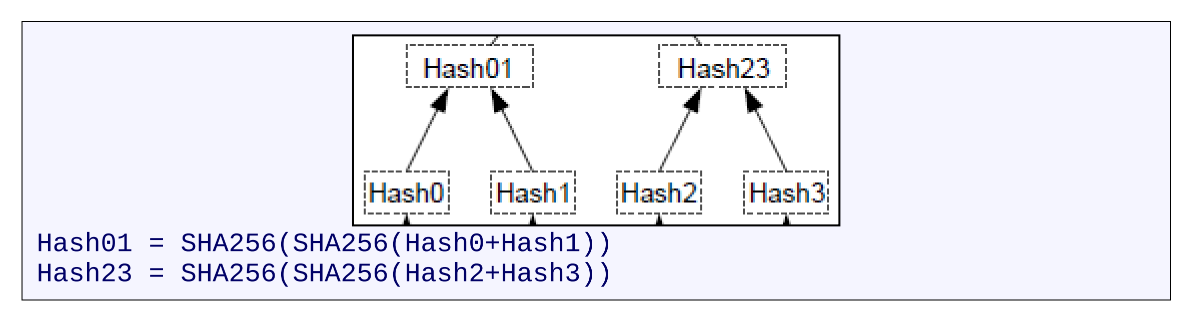
1. Hojas del árbol: Son los nodos del nivel inferior. Se calculan los hashes dobles de cada transacción que va a formar parte del bloque (es decir, SHA-256 del SHA-256 de la Transacción).

```
Hash0 = SHA256(SHA256(Tx0))
Hash1 = SHA256(SHA256(Tx1))
Hash2 = SHA256(SHA256(Tx2))
Hash3 = SHA256(SHA256(Tx3))
```

   a. Si el número de transacciones es impar, el último hash doble se duplica, para garantizar que los nodos son pares.

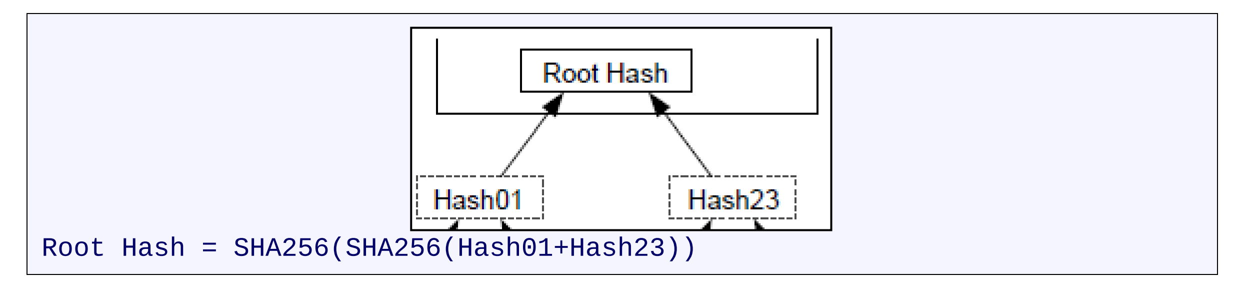
```
Hash3 = Hash2
```

2. Nodos intermedios: Los hashes calculados en el nivel inferior se agrupan por parejas y se calcula el hash doble correspondiente a la concatenación de dichos hashes. Este proceso se repite de forma recursiva, de manera que cada nivel tendrá la mitad de nodos que el nivel anterior.




```
Hash01 = SHA256(SHA256(Hash0+Hash1))
Hash23 = SHA256(SHA256(Hash2+Hash3))
```

3. Raíz: El único elemento en el nivel superior del árbol, que se llama **raíz Merkle**, y se calcula de la misma forma que las anteriores.




```
Root Hash = SHA256(SHA256(Hash01+Hash23))
```



ANEXO II – RESUMEN DE VULNERABILIDADES

CVE-ID	Impact	Date	Title	Description
2012-4684	High	01/03/2013	bitcoind / Bitcoin-Qt Alert Signature Handling Remote DoS	bitcoind and Bitcoin-Qt contain a flaw that may allow a remote denial of service. The issue is triggered during the handling of a specially crafted signature alert. This may allow a remote attacker to cause a consumption of CPU or RAM resources, which will crash the system.
2013-2292	High	30/01/2013	bitcoind / Bitcoin-Qt Signature Verification Crafted Transaction Handling Remote DoS	bitcoind and Bitcoin-Qt contain a flaw that may allow a remote denial of service. The issue is triggered during signature verification when handling a specially crafted transaction that contains a saturation of content that uses SHA-256 hashing. This may allow a remote attacker to cause a consumption of CPU resources and a crash for the system.
2012-1910	High	16/03/2012	Bitcoin-Qt for Windows Malformed Bitcoin Protocol Message Handling Remote Code Execution	Bitcoin-Qt 0.5.0.x before 0.5.0.5; 0.5.1.x, 0.5.2.x, and 0.5.3.x before 0.5.3.1; and 0.6.x before 0.6.0rc4 on Windows does not use MinGW multithread-safe exception handling, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted Bitcoin protocol messages.
2010-5141	High	29/09/2010	wxBitcoin / bitcoind Bitcoin Transaction Unspecified Script Opcode Parsing Remote Bitcoin Theft	wxBitcoin and bitcoind contain a flaw that is triggered when the Bitcoin transaction code does not properly handle script opcodes. This may allow a remote attacker to spend other users' bitcoins.
2010-5139	High	29/07/2010	wxBitcoin / bitcoind Bitcoin Transaction Parsing Remote Overflow Bitcoin Creation	wxBitcoin and bitcoind are prone to an overflow condition. The program fails to properly sanitize user-supplied input resulting in an integer overflow. With a specially crafted transaction, a remote attacker can potentially create an excessive amount of bitcoins.